# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/30

A1

(11) International Publication Number: **WO 00/51032**

(43) International Publication Date: 31 August 2000 (31.08.00)

(21) International Application Number: PCT/US00/04723

(22) International Filing Date: 25 February 2000 (25.02.00)

(30) Priority Data:
09/258,396 26 February 1999 (26.02.99) US

(71) Applicant: GARFINKLE LIMITED PARTNERSHIP II [US/US]; 133 East 62nd Street, New York, NY 10021 (US).

(72) Inventors: GARFINKLE, Norton; 133 East 62nd Street, New York, NY 10021 (US). YOUNG, Steven, J.; 78 Ridgewood Avenue, Stamford, CT 06907 (US).

(74) Agent: MARHOEFER, Laurence, J.; Lane, Aitken & McCann, 2600 Virginia Avenue, N.W., Washington, DC 20037 (US).

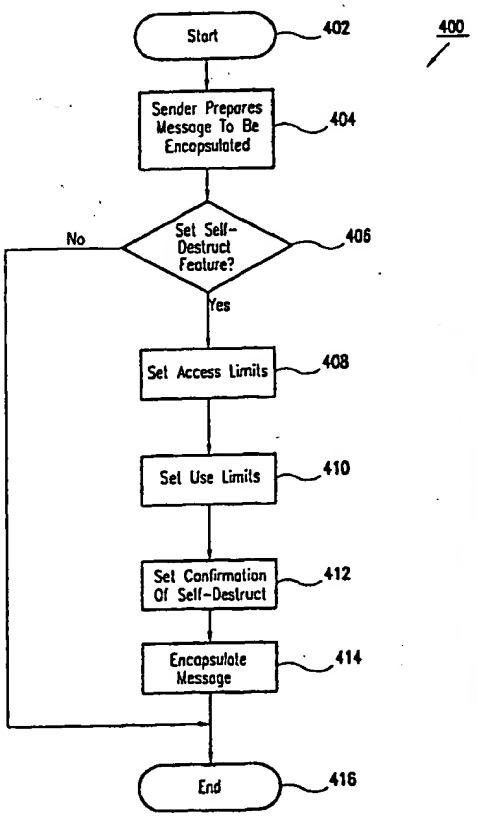
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR GENERATING A USER SELECTABLE SELF-DESTRUCTING E-MAIL

(57) Abstract

A system, method, and computer program product for enabling a sender to generate an E-mail including self-destructing, registered mail delivery and encryption features. The system, method and computer program product utilizing a technique including, for example, the steps of creating an E-mail with no content (402), attaching an attachment (404) to the E-mail, preparing a message including setting any of, for example, a self-destructive feature (406), a registered mail delivery feature and an encryption feature, encapsulating (414) the message in the attachment, and sending the E-mail with the attachment from the sender to the receiver.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | | | TR | Turkey |
| BG | Bulgaria | HU | Hungary | ML | Mali | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MN | Mongolia | UA | Ukraine |
| BR | Brazil | IL | Israel | MR | Mauritania | UG | Uganda |
| BY | Belarus | IS | Iceland | MW | Malawi | US | United States of America |
| CA | Canada | IT | Italy | MX | Mexico | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NE | Niger | VN | Viet Nam |
| CG | Congo | KE | Kenya | NL | Netherlands | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NO | Norway | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | NZ | New Zealand | | |
| CM | Cameroon | | | PL | Poland | | |
| CN | China | KR | Republic of Korea | PT | Portugal | | |
| CU | Cuba | KZ | Kazakstan | RO | Romania | | |
| CZ | Czech Republic | LC | Saint Lucia | RU | Russian Federation | | |
| DE | Germany | LI | Liechtenstein | SD | Sudan | | |
| DK | Denmark | LK | Sri Lanka | SE | Sweden | | |
| EE | Estonia | LR | Liberia | SG | Singapore | | |

# System, Method, and Computer Program Product for Generating A User Selectable Self-Destructing E-Mail

## *Background of the Invention*

### *Field of the Invention*

The present invention relates to electronic mail (E-mail) systems and more particularly, to functions selectable by a sender of E-mail messages.

### *Related Art*

Electronic mail, also known as E-mail, is a widely used means of communicating. A conventional E-mail system enables sending E-mail notes or E-mail messages much like a conventional postal letter. For example, a sender could send an E-mail message including text and a return E-mail address to a receiver at the receiver's E-mail address on another computer through the network connecting the computers. E-mail messages provide several advantages over conventional postal mail, such as, for example, faster delivery time, faster preparation time, savings from postage stamps and a more simple addressing scheme than using name, street address or post office box, city, state and zip code. However, conventional E-mail systems do not provide all the services available from conventional postal mail. For example, conventional E-mail systems do not provide the function of postal mail registered mail.

E-mail messages in early E-mail systems, included primarily text. Eventually, users were able to attach files for delivery along with the E-mail message. Such attached files are often called "attachments." Many E-mail systems support attaching multiple documents to an E-mail message.

Some E-mail systems use a centralized post office box. The post office box can be used to store a message from a sender which can then forward the message later to a temporarily disconnected addressed receiver. The centralized post office can also permit messages to be centrally backed up on a periodic basis.

Another type of E-mail system is a client/server E-mail system. With a client/server E-mail system, a portion of the E-mail generating program can reside on a client's computer (the computer of the sender or receiver), and another portion of the E-mail system can reside

on a server computer. E-mail application software can run on a variety of operating systems and computer system platforms.

Yet another type of client/server E-mail system is known as "groupware." Groupware enables functions in addition to the communication capability of E-mail including, for example, project management, location independent cooperation and information accessibility links.

Examples of E-mail systems include, for example, Lotus cc:Mail available from IBM, MS Mail available from MICROSOFT, PROFS and OFFICEVISION available from IBM, All-In-One from DEC and the Internet's Simple Mail Transfer Protocol (SMTP). Examples of groupware include Lotus Notes available from IBM, Exchange, available from MICROSOFT, Collabra Share, available from NETSCAPE and Groupwise, available from NOVELL.

Early E-mail systems implemented communication in a proprietary fashion. For example the systems were used for sending messages to users on an intranet system, with little consideration taken to interacting with other E-mail systems or networks. An intranet is a term often used to describe a stand alone network or group of networks which includes a related group of senders and receivers, such as, for example, the employees of a commercial company.

Some intranet E-mail systems are equipped to interoperate with other E-mail systems. Computers in a network communicate by using programs which in turn use a communication language or "protocol." Some E-mail systems are implemented using a so-called "open systems" communications method such as the transmission control protocol/ internet protocol (TCP/IP) suite of protocols. The TCP/IP protocol suite includes the SMTP E-mail functionality already mentioned. Many intranet E-mail systems were implemented using proprietary protocols for communication. Using a proprietary set of protocols, an intranet E-mail system could provide additional functions to its users. In time users wanted to communicate with other users who were not on their own intranet. With a lack of standards for implementing the additional functions provided to the intranet users, the use of those functions was lost when communicating with a user not on the intranet, such as, for example, a user on the Internet.

An internet (i.e. with a lower case "i") is a network which connects two separate networks. The global Internet (i.e. with a capitalized "I") is an internet that grew out of a U.S. Defense Advanced Research Projects Agency (DARPA) project. The Internet originally served a largely technical audience composed of the military, government agencies, and academic researchers and scientists. The original goals of the project were to allow researchers to share computing resources and to exchange information, regardless of their locations, and to create a resilient, fault-tolerant wide area network (WAN) for military communications. The global Internet implements communication using the TCP/IP communications protocols.

On-line service providers originally provided intranet E-mail system access to individuals via modem connections. On-line service providers include, for example, American

On Line (AOL), CompuServe, and Prodigy. Online services traditionally created offerings targeted toward home computer users. These providers often provided proprietary E-mail systems to connect their users to one another. In time, users on proprietary on-line services, were able to send messages to users on other E-mail services via the Internet.

During the mid-1990's, commercial enterprises and individuals increasingly discovered the benefits of being connected to the Internet, eventually creating a mass-market phenomenon. Today, although access is limited in some areas, most countries have ties to the Internet. Thus, the Internet enabled widespread, standardized intercommunication between users of disparate E-mail systems.

On-line services, in an effort to differentiate themselves from one another, and new low cost Internet mail providers, have sought to provide additional functionality to their E-mail systems to retain their subscribers and attract new ones. For example, AOL has added functionality to its E-mail program in order to permit a user to send a message including colored text, differing font sizes, and different fonts. Such textural highlighting can only be observed, by a recipient on the AOL on-line service. A recipient on another on-line service or using an Internet mail service, would only see the textual message.

Other intranet E-mail systems, such as a groupware system, for example, can provide additional functionality for recipients of E-mail created on their proprietary system. For example, the intranet E-mail system might support a sender's request for acknowledgment of the opening of a message on a computer of a recipient of the message. However, when the sender sends an E-mail message to a receiver who is not using the same E-mail system as the sender, the sender may lose the return receipt acknowledgment functions.

Thus, the means to enable receipt acknowledgment to a sender for an E-mail sent to a different E-mail system from that of the sender is desired.

Internet security issues are a source of widespread concern related to E-mail systems, although more security tools are presently available than ever before. Firewalls are more robust, administration and audit tools are more plentiful, and developing standard security procedures prevent most outside attacks while creating an audit trail for any that do get through. The growth of the use of the Internet for E-mail and the drive toward electronic commerce have generated significant interest in the development of standards for securing these environments. These environments share the common characteristic that they must operate between organizations, not just within a single organization, and often involve the use of networks that are themselves insecure. For example, in the mid 1990's the Secure Electronic Transaction (SET) standard for securing credit-card payments across the Internet was drafted. Other security related standards for securing E-mail messages are being developed such as, for example, PEM, S/MIME, PEM-MIME/MOSS, and PGP, and X.500

and X.509 for secure directory services. Although these standards are critical to secure communication, transactions and the deployment of electronic data interchange (EDI) and other applications that use the Internet, few are widely accepted or adopted today. Difficult choices remain as to which standard is more effective in solving security issues and which will become an accepted or an official standard in the future.

Unlike E-mail in a private system, which goes directly from the sender to the server and waits there until retrieved by the receiver, Internet E-mail moves from server to server on its way to the receiver. This process makes the transmission channel impossible to secure and provides numerous opportunities for interference. It has been conventionally thought that the only way to ensure E-mail privacy was to use encryption. As security related standards evolve and E-mail systems or services adopt such standards a more secure E-mail message will be able to be sent from a sender to a recipient. However, in the interim, no means exists to permit an E-mail message to be sent in a secure fashion from a sender to a receiver. Further, there is no provision for ensuring receipt by the intended receiver and preventing access to the message by an imposter with access to a receiver's E-mail mailbox. Thus, a means of securing a transmission of an E-mail being sent over the Internet between users on disparate systems is desired.

Conventional E-mail systems lack several other desirable functions when being used to send a message to a receiver over the Internet. For example, a sender of an E-mail is often concerned that the E-mail message will be initially sent to or later be forwarded to a recipient whom the sender does not wish to access or manipulate the message. No provision exists for verifying that the receiver is the intended recipient of the message, prior to divulging the contents of the E-mail. No provision exists to prevent forwarding of an E-mail sent over the Internet. Conventional E-mail systems do not enable a sender to send an E-mail to a receiver and enable the sender to designate that the recipient only be permitted to read the message, but not be able to perform certain functions with the message such as, for example, archive the message, print the message, or otherwise modify or manipulate the message.

Further, present systems do not enable a sender to require the E-mail message to automatically remove itself from the E-mail system of the recipient after a particular date and time or after a particular duration of time such as, for example, a time after sending, receipt, opening, reading, or closing following reading.

Also, conventional systems do not provide the sender the ability to require that the message become unreadable by anyone other than, or including, the receiver, after a particular date and time or duration. Conventional E-mail systems do not provide for such an E-mail retention system, comparable to a document retention system. In addition, an E-mail system

enabling self-destruction of E-mail messages upon satisfaction of certain criteria designated by a sender, receiver or other party is desired.

Conventional E-mail systems do not provide the means analogous to a "registered mail" feature of the postal mail system. For example, in the postal system, a sender can select registered mail and can require a signature of receipt in order for the receiver of the mail to access the contents of the mail. This signature is then sent back to the sender as proof of receipt by the recipient of the postal mail. The sender of an E-mail message over the Internet cannot currently receive a comparable signed acknowledgment of receipt of the sender's E-mail message.

Conventional E-mail systems also do not provide authentication of the sender to a receiver. Further, present E-mail systems do not provide authentication of the contents of the E-mail message to the receiver.

Thus, what is needed is an improved E-mail system which can perform additional functions, including, e.g., enabling a person to control access to and use of an E-mail, authenticating the sender, receiver and contents of the message, controlling retention of and requiring self-destruction of the E-mail message.

## *Summary of the Invention*

A method, system, and computer program product are provided that enable a user to generate an improved E-mail for sending to another user. In one embodiment of the invention, the E-mail can include various useful features, such as, e.g., self-destruction, registered mail, and encryption features. In an example embodiment, the technique can include the steps of creating an e-mail with no content, attaching an attachment to the e-mail, preparing a message including setting a self-destruct feature, a registered mail feature, and/or an encryption mail feature, encapsulating the message in the attachment, and sending the e-mail with the attachment from a sender to a receiver.

In another embodiment, the method can include a feature setting an access limit such as, e.g., limiting access to where no one can access the message after a time duration after an event, limiting access to where no one can access the message after an absolute date and time, and limiting access to where no one can access the message after a specified number of readings of the message, e.g., a single reading.

In another embodiment, the method can also include a feature setting a use limit such as, e.g., limiting use to where no one can print, archive, and cut/copy/paste the message.

Another embodiment includes a feature setting a confirmation of the self-destruction feature including, e.g., notifying the sender and receiver of self-destruction of the message.

In another embodiment, the method can also include receiving the e-mail with the attachment at the receiver's computer, opening the e-mail and attachment and activating attachment agents which can include, for example, activating a trip wire and a self-destruct agent, determining whether criteria are satisfied to reveal the message and revealing the message for viewing if the criteria are determined to be satisfied, including, for example, unencapsulating and unencrypting the message, enforcing use and access limits, and unrevealing the message after viewing is complete.

Another embodiment includes a feature determining if the access limits are exceeded and if so, instantiates the self-destruct agent including, e.g., overwriting the file containing the e-mail and the message, and sending confirmation of self-destruction to the sender and receiver if requested.

In another embodiment, the registered mail delivery feature can include setting a receipt acknowledgment preference such as, e.g., notification of receiver's receipt to the sender. The sender can also set a receiver verification requirement requiring entry of, e.g., a personal identification number (PIN), a fingerprint, a voiceprint, a digital signature, a retina scan, an other biometric confirmation, or a key. Self-destruct and trip wire E-mail features can be enabled. If a receiver does not satisfy a verification requirement, the E-mail can be set to automatically self-destruct, for example.

Further features and advantages of the invention, as well as the structure and operation of various embodiments of the invention, are described in detail below with reference to the accompanying drawings. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The drawing in which an element first appears is indicated by the leftmost digits in the corresponding reference number.

## *Brief Description of the Drawings*

The foregoing and other features and advantages of the invention will be apparent from the following, more particular description of a preferred embodiment of the invention, as illustrated in the accompanying drawings.

FIG. 1A is a block diagram of a distributed client/server E-mail system;

FIG. 1B is a block diagram of an exemplary system depicting an E-mail application program running on a computer hardware and operating system platform;

FIG. 2A depicts a conventional E-mail;

FIG. 2B depicts an improved E-mail of the present invention;

FIG. 3 is a flowchart illustrating a high level representation of an exemplary improved E-mail by a sender according to the present invention;

FIG. 4 is a flowchart illustrating an example of a sender setting the self-destruct feature of the E-mail of the present invention;

FIG. 5 is a flowchart illustrating an example of a sender setting the registered mail feature of the E-mail of the present invention;

FIG. 6 is a flowchart illustrating an example of a sender setting the encryption feature of the E-mail of the present invention;

FIG. 7 is an example flowchart illustrating an exemplary process of receiving and accessing the contents of an improved E-mail by a receiver according to the present invention;

FIG. 8 is an example flowchart illustrating a criteria satisfaction determination process of the exemplary process of receiving and accessing the improved E-mail by the receiver of the present invention;

FIG. 9 illustrates an example E-mail self-destruction process of the present invention;

FIG. 10 illustrates an example trip wire process of the present invention;

FIG. 11 illustrates a block diagram of an improved distributed client/server E-mail system including an exemplary user and E-mail verification system;

FIG. 12 is a flowchart illustrating an example process of a sender preparing an improved E-mail including an embedded unique public address and an embedded private identification according to the present invention;

FIG. 13 is an example flowchart illustrating an exemplary process of receiving and authenticating the contents of an improved E-mail by a receiver;

FIG. 14 is a flowchart illustrating an example process of a sender preparing an improved E-mail including an embedded unique public address and storing a private identification in a PID database according to the present invention;

FIG. 15 is an example flowchart illustrating an exemplary process by a receiver of receiving an improved E-mail and verifying a user before revealing the contents of the E-mail; and

FIG. 16 depicts an exemplary computer system of the present invention.

## *Detailed Description of the Invention*

The preferred embodiment of the invention is discussed in detail below. While specific implementations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without parting from the spirit and scope of the invention.

### *Overview of the Invention*

The present invention is directed to a system, method and computer program product that permits a sender to send an E-mail to a receiver over a communications network, where the E-mail includes additional embedded information and settings limiting the use and access to the message contents of the E-mail. In an embodiment of the invention, the message can be encapsulated within an attachment or an embedded object. A message reveal key can be used to unencapsulate the contents of the E-mail. The present invention can enable additional features such as, e.g., use of any of a self-destruction feature, an encryption feature, and a registered mail delivery feature.

A self-destruction feature including a self-destruct agent can be included in the E-mail. The self-destruct agent can be used to initiate destruction of the E-mail at a computer, such as, e.g., the receiver's computer, at a server, at the sender's computer and at any intervening computers. A trip wire agent can also be included in the E-mail. The trip wire agent can be used, e.g., to automatically set a self-destruct agent on a computer in order to cause the E-mail to destruct upon satisfaction of certain criteria set by the sender, or other user, authorized to enable the feature. The trip wire agent and self-destruct agent can include a computer program similar to a virus program which, upon satisfaction of certain criteria or occurrence of certain events, could automatically be instantiated and executed.

An encryption feature such as, e.g., a cryptographic algorithm and a hash digest, can be used to encrypt the contents of the message within the E-mail.

A registered mail delivery feature can be used to require a receiver to verify the receiver's identity prior to revealing the contents of the E-mail. A verification requirement and/or key can be used to require, e.g., entry of a cryptographic key, in order to gain access to the contents of the message in the E-mail.

The present invention provides additional features. For example, use limits can be set by the sender to limit the uses to which the receiver can use the E-mail. For example, the sender can set no limits to the use of the E-mail message. Alternatively, the sender can limit the use by the receiver. For example, the sender can disable printing of the E-mail including, for example, disabling screen capture while its contents are revealed. Other uses, could include, e.g., disabling archive and back-up of the E-mail, and disabling the capability of cutting/copying/pasting the contents of the E-mail.

Another feature provided by the present invention can be access limits. Access limits can be set by the sender in order to limit access by the receiver to the contents of the E-mail. For example, the sender can set an access limit to where no one can access the contents of the E-mail after a specific time duration. The time duration can include, e.g., days, hours, minutes, seconds, after a particular time, such as, e.g., after sending and/or creating the E-mail, and after the opening of/or receipt of the E-mail. The sender could also set an absolute

date or time after which no one could access the E-mail. In an alternative embodiment, particular access limits could be set for particular users, such as, for example, a specific access limit for a receiver, versus a different access limit for the recipient of a forwarded E-mail from the receiver. In another example access limit, access can be limited to where no one could access the contents of the E-mail after a specific number of readings of the message, such as, e.g. a single reading. Another access limit can provide no limits to access for the receiver.

Yet another feature permits confirmation of self-destruction of the E-mail. This feature can permit the sender to set a request to be notified upon self-destruction or automatic self-destruction of the E-mail. In another embodiment, confirmation of self-destruction can notify the receiver or another user of the self-destruction of the E-mail and/or destruction of the E-mail.

*An Example Embodiment of the Invention*

FIG. 1A illustrates a block diagram of E-mail system environment 100 which includes an exemplary distributed client/server computer E-mail system. E-mail system environment 100 includes a sender 102 which sends an E-mail message to a receiver 104. Sender 102 creates the E-mail on a client computer 106. Client computer 106 transmits the E-mail from sender 102 to receiver 104 on a client computer 110. An E-mail message may be created via mail client 116 of client computer 106 and may be sent via interaction with a mail server 118 on server 112 over a communications network 114. An E-mail 200, described further in relation to FIG. 2A below, in being sent from sender 102, can travel over communications network 114, and can pass through other computers, such as, e.g., a client computer 108, enroute to its final destination, client computer 110 for receipt by receiver 104. In one embodiment of the invention, communications network 114 includes an intranet. In another embodiment, communications network 114 includes the global Internet. It would be apparent to a person having ordinary skill in the art that the features of the present invention can be used in alternative E-mail system environments and architectures.

FIG. 1B depicts an exemplary computer environment 120 for client computer 106. It would be apparent to a person having skill in the art that environment 120 could also depict client computers 108 and 110 and server 112. Environment 120 includes hardware 122, operating system 124 and application programs 126, 128 and 130. Operating system 124 provides a uniform interface of application programming interfaces (APIs) to applications 126, 128 and 130 for access to hardware 122. An exemplary application 130 is an E-mail application program, mail program 134.. Mail program 134 is an example of mail client 116 and mail server 118. Alternatively, a mail program 132 can be included as part of operating system 124 to provide E-mail functionality to applications 126, 128 and 130.

FIG. 2A illustrates an example of a conventional E-mail 200. E-mail 200 includes various data components. Example data components included in E-mail 200, are creation information 202, a body 204, address information 206, a subject 208 and attachments 210 and 212.

In an example embodiment, creation information 202 can include, e.g., the date and time E-mail 200 was sent from sender102 to receiver 104. Body 204 of E-mail 200 can include, e.g., text 214 and embedded objects 216. Example embedded objects 216 can include attachments such as, for example, attachments 210 and 212. Other embedded objects 216 can include, e.g., bit map images, graphics objects, executable programs, compressed text and applets. Embedded objects 216 can also include a forwarded E-mail 200. Address information 206 can include the E-mail address of sender102 and receiver 104 of E-mail 200. Attachments 210 and 212 can also include other embedded objects 218. Subject 208 can include a brief description of the contents of E-mail 200. It would be apparent to persons skilled in the art that E-mail 200 can include a subset of the listed components, or additional components.

FIG. 2B illustrates an example implementation of the present invention, including improved E-mail 220. E-mail 220 can include components comparable to E-mail 200. In one embodiment, E-mail 220 includes creation information 222, a body 224, address information 226, a subject 228 and attachments 230 and 232. It is important to note that in one embodiment, body 224 of the improved E-mail 220 of the present invention includes a limited text portion 252 slightly different from text 214 of E-mail 200. In particular, text portion 252 of improved E-mail 220 merely explains that the message is in an attachment and does not include the contents of the message itself.

Attachment 230 further illustrates E-mail 220 of the present invention. The message portion of the E-mail is encapsulated within attachment 230. In particular, encapsulated E-mail 234 includes a conventional E-mail 200 with attachments 210 and 212 in an encapsulated form. In one embodiment of the invention, encapsulation can prevent a computer hacker from being able to detect the contents of the message portion of encapsulated E-mail 234. In another embodiment, encapsulation encrypts the contents of encapsulated E-mail 234.

Attachment 230 can include various other components. Attachment 230 can include, e.g., encryption information 236, verification key 238, trip wire agent 240, self-destruct agent 248, message reveal key 250, use limits 242, access limits 244 and a confirmation of self-destruct setting 246. E-mail 220 of the present invention can also include address information 226 such as, for example, the E-mail addresses of sender 102 and receiver 104 of E-mail 220.

The present invention enables sender 102 to send E-mail 220 to receiver 104 over communications network 114, where E-mail 220 includes additional embedded information and settings limiting the use of and access to the E-mail 220 itself. In another embodiment, another

user, such as, for example, the receiver 104, can set the limits to use of and access to E-mail 220, after receipt of E-mail 220 with a message in an attachment.

In an example embodiment, encryption information 236 can include information used to encrypt the contents of message text 204 within encapsulated E-mail 234 of attachment 230.

In one embodiment, verification key 238 can include information used to require entry of a cryptographic key, such as, e.g., a unique public address (UPA), a private identification (PID), a public or private key, a personal identification number (PIN), a signature, and an other biometric confirmation or identification, used in order to gain access to the message contents of encapsulated E-mail 234.

In one embodiment, trip wire agent 240 can include information used to automatically set a self-destruct agent 248 on client computer 110 of receiver 104. Self-destruct agent 248 could be used to cause E-mail message 220 to self-destruct upon satisfaction of certain criteria set by sender 102. In another embodiment, trip wire agent 240 can be set by receiver 104 or another user to effect destruction of E-mail 220. A person skilled in the art will appreciate that trip wire agent 240 in one embodiment can be a so-called virus or trojan horse application program.

In one embodiment, self-destruct agent 248 of E-mail 220 upon instantiation of the program object can be used to initiate destruction of E-mail 220 at computer 110 of receiver 104. In another example embodiment, self destruct agent 248 can be used to destroy E-mail 220 upon satisfaction of criteria such as, e.g., attempting to open E-mail 220 after a particular time duration measured by comparing the time value of creation information 222 with that of system clock of client computer 110 or the results of a query to a secure time server on a server 112 on communications network 114. In another embodiment, self-destruct agent 248 can be used to destroy E-mail 220 on other computers 106, 108 and 112. Trip wire agent 240 and self-destruct agent 248 can include, for example, a computer program similar to a virus program which, upon occurrence of certain events or satisfaction of certain criteria could automatically be instantiated and executed.

In an embodiment of the invention, message reveal key 250 can be used to reveal the contents of E-mail 220. In particular, message reveal key 250 can perform functions including unencapsulating the encapsulated E-mail message 234.

Use limits 242 in one embodiment of the invention can be set by sender 102 to limit the kinds of uses to which receiver 104 can use E-mail message 220. For example, sender 102 can choose to set no limits to the use of E-mail message 220. Alternatively, sender 102 can limit the use by receiver 104 to, for example, disabling printing of the message in E-mail 220. Disabling printing can include, for example, disabling screen capture while message text 204 of encapsulated E-mail 234 is displayed. Other uses, could include disabling the ability to

archive or make back-ups of E-mail 220, and disabling the capability of cutting/copying/pasting the contents of encapsulated E-mail 234, i.e., message text 204. In another embodiment, other users, such as, e.g., receiver 104 can set use limits 242 for E-mail 220. For example, sender 102 can send E-mail 220 with a message in attachment 230 to receiver 104, and then receiver 104 or another user can set use limits 242 for E-mail 220.

Access limits 244, in one embodiment, can be set by sender 102 in order to limit access to the contents of E-mail 220. In particular, for example, sender 102 can set an access limit to where no one, or only receiver 104 for example, can access E-mail message 220 after a specific time duration. A specific time duration can be set, for example, in days, hours, minutes, seconds. The time duration can be calculated from occurrence of a particular event, such as, for example, after sending or creation of E-mail message 220, after the opening of or receipt of E-mail 220 by receiver 104, after no access to the message for a period of time, or after an attempted unauthorized access to the message. Instead of a time duration, sender 102 could set an absolute date and time, after which no one could access E-mail 220. It would be apparent to persons skilled in the art that various methods could be used by a computer to determine the passage of a time duration or occurrence of an absolute date/time, such as, e.g., querying the computer's system clock or a secure time server. In an alternative embodiment, multiple access limits 244 could be set for different particular users, such as, for example, a specific access limit for receiver 104, versus a different access limit for the recipient of a forwarded E-mail from receiver 104. Another example access limit could limit access to where no one could access E-mail 220 after a specific number of readings, such as, e.g., a single reading of message text 204. Another access limit could provide no limits to access E-mail 220 for receiver 104, or another user. In another embodiment, other users, such as, e.g., receiver 104 can set access limits 244 for E-mail 220. For example, sender 102 can send E-mail 220 with a message in attachment 230 to receiver 104, and then receiver 104 or another user can set access limits 242 for E-mail 220.

In an embodiment of the invention, confirmation of self-destruct setting 246 can permit a sender to request notification of self-destruction of E-mail 220. In another embodiment of the present invention, confirmation of self-destruct setting 246 can notify receiver 104 of self-destruction of E-mail 220. Confirmation can include additional information such as the time of destruction, the reasons for destruction, and other useful attributes of E-mail 220.

FIGs. 3-6 below illustrate an example embodiment of the present invention including preparation of E-mail 220 from the viewpoint of sender 102.

FIG. 3 includes flowchart 300. Flowchart 300 begins with step 302 and proceeds immediately to step 304. In step 304, a sender prepares an E-mail with no message content which states that a message, i.e. encapsulated E-mail 234, is in the attachment, i.e. attachment

230. Step 304 also includes preparation by sender 102 of attachment 230. From step 304, flowchart 300 continues with step 306, where sender 102 prepares a message including message text 204 and encapsulates the message in attachment 230 as encapsulated E-mail 234. Flowchart 300 continues from step 306 to step 308. In step 308, sender 102 sends E-mail 220 to receiver 104. The message can be sent from client computer 106 to client computer 110 over communication network 114. Flowchart 300 continues from step 308 with step 310 where the process ends. Step 306 of flowchart 300 can include any of various sub-processes, as depicted in FIGs. 4-6, 12 and 14, below.

FIG. 4 illustrates an example sub-process that can optionally be included in step 306 of FIG. 3. FIG. 4 depicts flowchart 400. Flowchart 400 starts at step 402 and proceeds immediately to step 404. In step 404, sender 102 prepares message 204 to be encapsulated as encapsulated E-mail 234. Flowchart 400 continues with step 406. In step 406, sender 102 can decide to set self-destruct feature enabling self destruction of E-mail 220. If sender 102 chooses not to set the self-destruct feature in step 406, flowchart 400 proceeds immediately to step 416 and ends. However, if sender 102 chooses to set the self-destruct feature in step 406, flowchart 400 continues with step 408. In step 408, access limits 244 can be set. Access limits 244 include those described above with reference to FIG. 2B.

Examples of access limits 244 include, e.g., no limit to access and limits to access. Limits to access enforced against receiver 104, or another user, can include, e.g., a limit to where no one can access E-mail 220 after a duration of time or after an absolute date and time, and a limit where no can access after a specific number of readings, such as, e.g., a single reading of the contents of E-mail 220. Time durations can be measured, e.g., in months, weeks, days, hours, minutes and seconds. An access limit 244 time duration can be measured from any date and time, or occurrence of an event. Events bounding a time duration can include, e.g., creation of, sending of, receipt by the computer of, receipt by the receiver of, opening of, reading of, and closing of E-mail 220. Access limits 244 can be set at an absolute date and time or occurrence of some event including the events bounding time durations. Date and/or time can be calculated by interaction with the computer's system clock. Date and/or time can also be determined by another technique of determining the time such as, e.g., a query to a server 112 computer configured to provide the time, preferably providing the time in a secure, reliable fashion.

From step 408, flowchart 400 continues with step 410. In step 410, use limits 242 can be set. Use limits 242 are introduced with reference to FIG. 2B above.

Examples of use limits 242 include, e.g., no limit to use and limits to use. Limits to use enforced against receiver 104, or another user, can include, e.g., not permitting printing of, not permitting archive or backup of, not permitting cut and copy from and paste to, E-mail

220. To not permit printing, screen capture should be disabled when the message is revealed. Interaction between the E-mail system application program 130 and 134 and operating system 124 can be used to enable enforcement of use limits 242.

From step 410, flowchart 400 continues with step 412. In step 412 confirmation of self-destruct can be set so as to notify a sender 102 or receiver 104,or other user, of the self-destruction of E-mail 220. From step 412, flowchart 400 continues with step 414. In step 414, message 200 is encapsulated into E-mail 220 as encapsulated E-mail 234. From step 414, flowchart 400 ends with step 416.

FIG. 5 illustrates another example embodiment of the present invention. FIG. 5 includes flowchart 500 which can be an optional sub-process of step 306 of FIG. 3. Flowchart 500 begins with step 502 and proceeds immediately to step 504. In step 504, sender 102 prepares an E-mail message 200 to be encapsulated as encapsulated E-mail 234. From step 504, flowchart 500 continues with step 506. In step 506, sender 102 can choose to set a registered mail feature. The registered mail feature enables functionality comparable to the registered mail feature of the postal system. For example, the registered mail feature can provide acknowledgment of receipt by, e.g., receiver 104, client computer 110 and an authorized or verified representative of receiver 104. Various levels of security and enforcement can be required and enforced. For example, receiver 104 can be required to enter a code in order to access E-mail 220.

In step 506, if sender 102 chooses not to set the registered mail feature, flowchart 500 continues with step 516, immediately ending the process. In step 506, if sender 102 chooses to set the registered mail feature, then flowchart 500 continues with step 508.

In step 508, sender 102 can choose to set a receipt acknowledgment preference. A receipt acknowledgment preference can include, e.g., sending a message to sender102 acknowledging opening of attachment 230 by receiver 104 or another user, sending a message to sender 102 acknowledging receipt at client computer 110. From step 508, flowchart 500 continues with step 510.

In step 510, verification requirements can be set. A verification requirement can include, for example, no verification to be required, or a specific verification to be required. A specific verification can include, e.g., entry of a personal identification number (PIN), use of a fingerprint verification, use of a voice print verification, a retina scan, a digital signature, an other biometric confirmation or identification, and a key such as, e.g., a private key or a public key. From step 510, flowchart 500 continues with step 512.

In step 512, sender 102 can choose to set a secured transmission preference. A secured transmission preference can include setting a variety of security levels. Secured transmission preferences can include limiting access to particular individuals such as, for example, receiver

104, or an authorized representative of receiver 104. In one embodiment, a secured transmission preference can require one or more verifications and/or authentications and/or levels of encryption.

In step 512, sender 102 can also set access limits 244. Access limits 244 control access to the contents of E-mail 220 by a user. See the discussion of access limits in FIGs. 2B and 4 above. Access limits 244 can be used to limit access to particular individuals or to set no limit to access. Access limits 244 can include limiting access to the file to where no one can access E-mail 220 after a given time duration or after an absolute date and time. A time duration can, for example, include a time after the sending or creation of an E-mail or after the opening or receipt of E-mail 220 by receiver 104. A time duration can be set, for example, in days, hours, minutes and seconds. In another embodiment, access to the contents of E-mail 220 can be limited to where no one can access the contents after a specific number of readings, such as, e.g., a single reading of E-mail 200 in encapsulated E-mail 234. Alternatively, access limits 244 can be set by receiver 104, or another authorized user, following receipt of E-mail 220.

Also, in step 512, use limits can be set by sender 102 to control usage of E-mail 220 by, e.g., receiver 104. Use limits 242 of 512 have been described with reference to FIGs 2B and 4 above and can include setting no limits as to use of E-mail 220. Use limits 242 can also be set by sender 102 to control the uses that receiver 104 can make with E-mail 220. For example, sender 102 can set that receiver 104 cannot print E-mail 220. Sender 102 can also set that receiver 104 cannot archive or save additional copies or forward copies of E-mail 220 to others. Further, sender 102 can, e.g., choose to disable the capability of cutting, copying, and pasting the contents of E-mail 220 into other computer programs. It would be apparent to a person having ordinary skill in the art that setting a use limit 242 to prevent printing of the message included in E-mail 220, can include disabling screen capture while the contents of E-mail message 220 is being displayed. Alternatively, use limits 242 can be set by receiver 104, or another authorized user, following receipt of E-mail 220.

The present invention could be used to enforce other secured transmission preferences, access and use limits, as well. From step 512, flowchart 500 continues with step 514 which encapsulates the E-mail message 220 and proceeds to step 516 where flowchart 500 ends.

FIG 6 illustrates an exemplary encryption process depicted in flowchart 600 which can optionally be included as part of step 306 of FIG. 3. Flowchart 600 starts with step 602 and proceeds immediately to step 604.

In step 604, sender 102 prepares a message to be encapsulated. From step 604, flowchart 600 continues with step 606.

In step 606, sender 102 has the option of setting that the message included in E-mail 220 be encrypted. If sender 102 chooses not to encrypt the message in E-mail 220, flowchart 600 continues immediately with step 612 where it ends.

In step 606, if sender 102 chooses to encrypt the message included in E-mail 220, flowchart 600 continues with step 608 which encrypts the message. Well known encryption methods can be used to encrypt E-mail message 200 in E-mail 220, including, for example, the use of hash digests and keys. It would be apparent to persons having ordinary skill in the art that a variety of encryption methods can be used to encrypt the contents of the message portion of E-mail 220. From step 606, flowchart 600 proceeds to step 610 which encapsulates the message before ending with step 612.

Other embodiments of the process of generating E-mail 220 of the present invention include any combination of the processes disclosed in FIGS. 3-6. For example, an E-mail system according to the present invention can include the encapsulation, self-destruction, encryption and registered mail features, and any subset thereof.

FIGs. 7 and 8 below further describe operation of the present invention including receiving and revealing a message from the viewpoint of receiver 104.

FIG. 7 illustrates flowchart 700 which depicts an exemplary embodiment of the present invention illustrating an example process of receiving E-mail 220 from the point of view of receiver 104. Flowchart 700 begins with step 702 which proceeds immediately to step 704. In step 704, client computer 110 of receiver 104 receives E-mail 220 containing textual portion 252, described with reference to FIG. 2B, containing no message content and stating merely that a message is encapsulated in attachment 230 along with E-mail 220. From step 704, flowchart 700 continues with step 706.

In step 706, receiver 104 opens E-mail 220 and initiates opening of attachment 230. From step 706, flowchart 700 continues with step 708. In step 708, attachment 230 activates several attachment agents. For example, trip wire agent 240 and self-destruct agent 248 can be activated. Activation of these agents can include instantiating a program object and/or scheduling execution of a program application thread or process. From step 708, flowchart 700 continues with step 710.

In step 710, decision logic is processed to determine whether the criteria are satisfied in order to reveal the contents of the message portion of E-mail 220. If the criteria are satisfied in step 710, processing of flowchart 700 continues with step 712, otherwise, processing ends and continues immediately with step 720 ending flowchart 700.

In step 712, the message portion of E-mail 220 is unencapsulated in order to reveal the message to receiver 104. From step 712, flowchart 700 continues with step 714.

In step 714, use limits and/or access limits as set previously by sender 102 are established and enforced. From step 714, flowchart 700 continues with step 716.

In step 716, receiver 104 can read the message contained in E-mail 220 and, when finished, can proceed to close the message. From step 716, flowchart 700 can continue with step 718.

In step 718, after receiver 104 closes the message, the contents are automatically re-encapsulated into attachment 230. In one embodiment, if the message is left open for a specific period of time, e-mail 220 can, e.g., automatically close itself and/or can initiate self destruction. Re-encapsulation requires placing the message back in the form it was in when it was received by client computer 110 of receiver 104. Following step 718, flowchart 700 ends with step 720.

FIG. 8 depicts an exemplary flowchart 710 corresponding to an example decision step 710 of FIG. 7. It should be apparent to a person having ordinary skill in the art that other decision steps 710 could be used. In another embodiment of the invention, a subset of the criteria whose satisfaction is determined in FIG. 8 are determined. FIG. 8 includes flowchart 710 beginning with step 802. FIG. 8 continues immediately from step 802 to decision step 804 which determines whether an access limit has been exceeded. In step 804, if an access limit has been exceeded, flowchart 710 continues with step 806 and if access limits 244 have not been exceeded, continues with step 808.

In step 806, self-destruct agent 248 can be instantiated. An exemplary embodiment of step 806 is explained further with respect to FIG. 9 below.

In step 808, satisfaction of verification requirement 238 criteria is determined. If verification requirements 238 have been satisfied, then flowchart 710 continues with step 812 and if the requirement has not been satisfied, then continues with step 810.

In step 810, it is determined whether an auto self-destruct feature has been selected in step 406 and, if so, flowchart 710 proceeds immediately to step 806. If, however, the auto self-destruct feature has not been selected in step 406, the flowchart continues with step 822. Verification requirements 238 can include no verification and a specific verification requirement, such as, for example, entry of a PIN, a fingerprint ID, a voice print, a retina scan, a digital signature and a key (e.g., public or private encryption/decryption key). An exemplary verification requirement is explained further with respect to FIG. 11 and flowcharts 12 through 15 below.

In step 812, it is determined whether the message in E-mail 220 has been encrypted and, if so, flowchart 710 proceeds to step 814, otherwise, it continues with step 818. In step 814, it is determined whether the encryption key has been satisfied and, if so, it proceeds to un-encrypt or decrypt the message in step 816. However, if the encryption key has not been

satisfied in step 814, flowchart 710 continues with step 822. From step 816, flowchart continues to step 818.

In step 818, it is determined whether the receipt acknowledgment has been requested in step 508. If a receipt acknowledgment has been requested, flowchart 710 continues with step 820 and, if not, flowchart 710 branches from step 818 to step 824. In another embodiment of step 818, a message can be sent to sender 102 acknowledging the opening of attachment 230 by receiver 104. Alternatively, an acknowledgment can be sent to another party who has requested acknowledgment of receipt.

In step 820, an acknowledgment of receipt by receiver 104 can be sent to sender 102 and flowchart 710 continues with step 824.

In step 822, it can be determined that the criteria have not been satisfied and flowchart 710 proceeds to end with step 826.

In step 824, it can be determined that criteria have been satisfied and flowchart 710 ends with step 826.

FIG. 9 depicts a flowchart 806 illustrating an example embodiment of self-destruct process of the present invention that could be performed by self-destruct agent 248. Flowchart 806 begins with step 902 and proceeds immediately to step 904.

In step 904, self-destruct agent 248 overwrites the file containing E-mail 220 on client computer 110 of receiver 104 and removes the file attributes table entries so as to render impossible access to the file containing E-mail 220 and its encapsulated message including message text 204. From step 904, flowchart 806 continues with step 906.

In step 906, receiver 104 is notified of self-destruction of E-mail 220 if confirmation has been requested by sender 102 in step 412. Flowchart 806 continues with step 908.

In step 908, sender 102 is notified of self-destruction of E-mail 220 assuming that sender 102 has requested confirmation of self-destruction. After sending the requisite confirmation of self-destruction, self-destruct agent 248 ends with step 910.

FIG. 10 depicts a flowchart 1000 illustrating an example embodiment of a trip wire process which instantiates trip wire agent 240 and self-destruct agent 248. Flowchart 1000 begins with step 1002 and proceeds immediately to step 1004.

In step 1004, trip wire agent 240 is triggered upon occurrence of an event. In step 1004, the triggering event that instantiates trip wire agent 240 can include, for example, the booting, i.e. start up, of the computer on which trip wire agent 240 resides. Another triggering event could include the occurrence of the value of the computer's system clock exceeding an access limit 244. It would be apparent to a person having ordinary skill in the art that trip wire agent 240 could include a thread or scheduled execution instance of a program that could reside commonly with the computer containing E-mail 220, e.g. client computer

110. In another embodiment of the present invention, trip wire agent 240 is triggered upon an alternative occurrence such as, for example, an unauthorized attempt to open E-mail 220 following expiration of access limit 244, or attempted use of the file unauthorized by use limits 242. Flowchart 1000 continues from step 1004 with step 1006.

In step 1006, self-destruct agent 248 can be instantiated. In one embodiment, the process of flowchart 806 of FIG. 9 can be performed. From step 1006, flowchart 1000 ends with step 1008.

FIG. 11 illustrates an exemplary environment requiring user verification by sender 102 and/or receiver 104 of the present invention. In particular, FIG. 11 depicts block diagram 1100 which expands upon block diagram 100 of FIG. 1A. Block diagram 1100 illustrates sender 102 sending an E-mail 2200 to receiver 104 over communications network 114 (not pictured) which can interact with server 112 and a private ID database 1106 to perform verification 238 and authentication functions. In block diagram 1100, sender 102 communicates via client computer 106 and receiver 104 communicates via client computer 108 as depicted by lines 1110 and 1112, respectively. In one embodiment, sender 102 and receiver 104 can provide input of a private ID into client computers 106 and 108 via private ID input devices 1102 and 1104, respectively. Alternatively, a private ID can be input via another device, such as, e.g., client computers 106 and 108.

In particular, sender 102 can input a private ID such as, e.g., a personal ID number, a fingerprint, a voice print, a retina scan, a signature and a key, via optional private ID input device 1102 into client computer 106 as represented by lines 1136 and 1138. Similarly, receiver 104 can also provide a private ID input into client computer 108 as represented by lines 1128 and 1130. Client computer 106 intercommunicates with server 112 and client computer 108 as represented by lines 1114, 1120 and 1132. Sender 102, prior to sending an E-mail 220 to receiver 104, can attach to E-mail 220 a unique public address (UPA).

The UPA can be used to control access, by receiver 104, to the message encapsulated in E-mail 220. For example, in one embodiment of the present invention, only receiver 104, is permitted to open the message. For receiver 104 to open the message, receiver 104 enters a private ID via optional private ID input device 1104 into client computer 108 and client computer 108 transfers the inputted private ID to server 112 as represented by line 1132. Server 112 then can transfer the private ID of receiver 104 to the validate ID input comparator 1108, as represented by line 1118.

Meanwhile, the UPA entered by sender 102 into client computer 106 can be sent along with E-mail 220 to server 112 as represented by line 1114, and the UPA can be forwarded to private ID database 1106, as represented by line 1116. In an alternative embodiment, private ID database 1106 can be included as part of server 108. Private ID database 1106 can be

queried to ensure that the proper addressee is attempting to access the message encapsulated in E-mail 220. A query can cause a database look-up using the UPA as an index to determine the correct addressee, i.e., the private ID of receiver 104, and can output this value to validate ID input 1108, as represented by line 1122.

Validate ID input 1108 can then compare the value of the private ID input by receiver 104 and the output of the private ID database 1106 database look-up. If the private ID entered by receiver 104 matches the results of the private ID database look-up, receiver 104 can be permitted to view of the contents of the message, so client computer 108 is instructed by validate ID input 1108 to reveal the message, as represented by step 1124.

In addition, in one embodiment, sender 102 can be notified of receipt of message 220 by receiver 104, as represented by line 1126. In another embodiment, sender 102 can include an identification of the sender which can be received by receiver 104 and used in a similar manner to authenticate that E-mail message 220 was created by sender 102.

FIG. 12 illustrates additional verification steps from a sender's point of view. In particular, FIG. 12 depicts flowchart 1200 illustrating an exemplary embodiment of the verification key process in greater detail. Flowchart 1200 in one embodiment is a portion of step 306 of FIG. 3. Flowchart 1200 begins with step 1202 and continues immediately with step 1204.

In step 1204, sender 102 prepares a message to be encapsulated. Flowchart 1200 continues with step 1206.

In step 1206, a unique public address (UPA) of sender 102 and/or receiver 104 is embedded in attachment 230. Flowchart 1200 continues with step 1208.

In step 1208, private identification (PID) of sender 102 and/or receiver 104 is embedded in attachment 230. Flowchart 1200 continues with step 1210.

In step 1210, the message is encapsulated and flowchart 1200 ends with step 1212. FIG. 13 below depicts receipt of E-mail 220 created according to the process detailed in FIG. 12.

FIG. 13 illustrates an exemplary use of a key verification from the receiver's point of view. FIG. 13 includes flowchart 1300. Flowchart 1300 begins with step 1302 and continues immediately with step 1304. In step 1304, receiver 104 receives E-mail 220. Flowchart 1300 continues with step 1306.

In step 1306, it is determined whether the PID of sender 102 and the UPA as attached to E-mail 220 by sender 102 in step 1206, match by performing a look-up in the private ID database of block 1106. If the PID and UPA are found to match by validate ID input 1108 in step 1306, flowchart 1300 continues with step 1308. If the PID and UPA do not match, flowchart 1300 continues with step 1310.

In step 1308, receiver 104 receives an authentication message from validate ID input 1108 as depicted by line 1124 in FIG. 11 and flowchart 1300 ends with step 1312.

In step 1310, receiver 104 does not receive an authentication message and can assume the message was not authenticated, and thus could possibly be corrupt and/or being sent from an imposter who is not sender 102. Flowchart 1300 continues from step 1310 with step 1312.

FIG. 14 illustrates another exemplary embodiment of the use of the unique public address (UPA) of the present invention. FIG. 14 includes flowchart 1400 depicting an embodiment of the present invention illustrating an optional portion of step 306 illustrated in FIG. 3 above. Flowchart 1400 begins with step 1402 and proceeds immediately to step 1404.

In step 1404, sender 102 prepares a message 200 to be encapsulated as encapsulated E-mail 234 in E-mail 220. Flowchart 1400 continues with step 1406.

In step 1406, the unique public address (UPA) of receiver 104 is embedded in attachment 230 of E-mail 220. Flowchart 1400 continues with step 1408.

In step 1408, private identification (PID) of receiver 104 is stored in PID database 1106. Flowchart 1400 continues with step 1410.

In step 1410, the message 200 prepared in step 1404 is encapsulated as encapsulated E-mail 234 and flowchart 1400 ends with step 1412. In one embodiment encapsulation includes a process of encryption. In another embodiment, encapsulation makes the contents of encapsulated E-mail 234 not easily accessible by a computer hacker. In another embodiment, encapsulation can perform an encoding process, or a process including a hash digest. FIG. 15 below illustrates, from a receiver's standpoint, use of the UPA of FIG. 14.

FIG. 15 illustrates flowchart 1500 depicting an example process of receiver 104 receiving E-mail 220 prepared by sender 102 in FIG. 14. Flowchart 1500 begins with step 1502 and proceeds immediately to step 1504.

In step 1504, receiver 104 receives E-mail 220. Flowchart 1500 continues with step 1506.

In step 1506, receiver 104 can enter a personal ID number (PID) associated with receiver 104 via an optional private ID input device 1104. Alternatively, a personal ID number can be entered via another well known means of data entry. Flowchart 1500 continues with step 1508.

In step 1508, it is determined whether the personal ID input by receiver 104 matches a personal ID stored in private ID database 1106 and, if they do match, flowchart 1500 continues with step 1510. Otherwise, if the PID and the PIP stored in private ID database 1106, do not match, flowchart 1500 continues with step 1512.

In step 1510, the criteria are satisfied to reveal the message so encapsulated message 234 in E-mail 220 can be revealed and flowchart 1500 ends at step 1514.

In step 1512, the required criteria have not been satisfied and so the contents of E-mail 220 are not revealed to receiver 104 and flowchart 1500 ends with step 1514.

In another embodiment of the invention, E-mail message 220 is transmitted via communications network 114 through a series of other servers 112. In another embodiment of the present invention, trip wire agent 240 and self-destruct agent 248 can remain attached to any new version of message 220 derived from it by further processing such as, for example, forwarding E-mail 220 and replying to E-mail 220.

The present invention is computer platform independent. Client computer 106 in a preferred embodiment is a personal computer (PC) system running an operating system such as Windows 98 Mac/OS, or a version of UNIX. However, the invention is not limited to these platforms. Instead, the invention can be implemented on any appropriate computer system running any appropriate operating system, such as, for example, Solaris, Irix, Linux, HPUX, OSF, Windows 98, Windows NT, OS/2, Mac/OS. In one embodiment, the present invention is implemented on a computer system operating as discussed herein. In another embodiment, the present invention can be implemented on hardware such as a handheld device, such as, e.g., a two-way pager, a cellular phone, a digital phone, a watch, a wireless device, a laptop, notebook or subnotebook computer, and other computer type device such as, e.g., a micro-computer, a mini-computer and a mainframe computer.

FIG. 16 depicts an exemplary client computer 106 computer system. Other components of the invention, such as client computer 108, private ID input devices 1102 and 1104, private ID database 1106 and/or server computer 110, could also be implemented using a computer such as that shown in FIG. 16.

The computer system 106 includes one or more processors, such as processor 1602. The processor 1602 is connected to a communication bus 1604. Client computer 106 also includes a main memory 1606, preferably random access memory (RAM), and a secondary memory 1608. The secondary memory 1608 includes, for example, a hard disk drive 1610 and/or a removable storage drive 1612, representing a floppy diskette drive, a magnetic tape drive, a compact disk drive, etc. The removable storage drive 1612 reads from and/or writes to a removable storage unit 1614 in a well known manner.

Removable storage unit 1614, also called a program storage device or a computer program product, represents a floppy disk, magnetic tape, compact disk, etc. The removable storage unit 1614 includes a computer usable storage medium having stored therein computer software and/or data, such as an object's methods and data.

Client computer 106 also includes an input device such as (but not limited to) a mouse 1616 or other pointing device such as a digitizer, and a keyboard 1618 or other data entry device.

Computer programs (also called computer control logic), including object oriented computer programs, are stored in main memory 1616 and/or the secondary memory 1618 and/or removable storage units 1614, also called computer program products. Such computer programs, when executed, enable the computer system 106 to perform the features of the present invention as discussed herein. In particular, the computer programs, when executed, enable the processor 1602 to perform the features of the present invention. Accordingly, such computer programs represent controllers of the computer system 106.

In another embodiment, the invention is directed to a computer program product comprising a computer readable medium having control logic (computer software) stored therein. The control logic, when executed by the processor 1602, causes the processor 1602 to perform the functions of the invention as described herein.

In yet another embodiment, the invention is implemented primarily in hardware using, for example, one or more state machines. Implementation of these state machines so as to perform the functions described herein will be apparent to persons skilled in the relevant arts.

While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

## *What is Claimed is:*

1. A method for enabling a sender to generate a self-destructing E-mail for sending to a receiver, the method comprising the steps of:

(1) creating an E-mail with no content;

(2) attaching an attachment to said E-mail;

(3) preparing a message including setting a self-destruct feature;

(4) encapsulating said message in said attachment; and

(5) sending said E-mail with said attachment from the sender to the receiver.

2. The method according to claim 1, wherein step (3) comprises the step of:

(a) setting an access limit including at least one step of the following steps:

(i) limiting access to where no one can access said message after a time duration after an event,

(ii) limiting access to where no one can access said message after an absolute date and time, and

(iii) limiting access to where no one can access after a specific number of readings of said message.

3. The method according to claim 1, wherein step (3) comprises the step of:

(b) setting a use limit including at least one step of the following steps:

(iv) limiting use to where no one can print said message,

(v) limiting use to where no one can archive said message, and

(vi) limiting use to where no one can cut/copy/paste said message.

4. The method according to claim 1, wherein step (3) comprises the step of:

(c) setting a confirmation of self-destruct feature including at least one step of the following steps:

(vii) notifying the sender of self-destruction of said message, and

(viii) notifying the receiver of self-destruction of said message.

5. The method according to claim 1, further comprising the steps of:

(6) receiving said E-mail with said attachment at a receiver's computer;

(7) opening said E-mail;

(4) opening said attachment and activating attachment agents including at least one step of the following steps:

(d) activating a trip wire agent, and

(e) activating a self-destruct agent;

(9) determining whether criteria are satisfied to reveal said message; and

(10) revealing said message for viewing if said criteria in step (9) are determined to be satisfied including at least one step of the following steps:

(f) unencapsulating said message,

(g) enforcing use limits, and

(h) enforcing access limits, and

unrevealing said message after viewing is complete.

6. The method according to claim 5, wherein step (9) comprises the steps of:

(j) determining if said access limits are exceeded; and

(k) instantiating said self-destruct agent if said access limits are determined to be exceeded in step (j), including at least one step of the following steps:

(ix) overwriting file containing said E-mail and said message,

(x) sending confirmation of self-destruction to the sender if requested, and

(xi) sending confirmation of self-destruction to the receiver if requested.

7. A method for enabling a sender to generate a registered mail delivery E-mail for sending to a receiver, the method comprising the steps of:

(1) creating an E-mail with no content;

(2) attaching an attachment to said E-mail;

(3) preparing a message including setting a registered mail delivery feature;

(4) encapsulating said message in said attachment; and

(5) sending said E-mail with said attachment from the sender to the receiver.

8. The method according to claim 7, wherein step (3) comprises the step of:

(a) setting an access limit including at least one step of the following steps:

(i) limiting access to where no one can access said message after a time duration after an event,

(ii) limiting access to where no one can access said message after an absolute date and time, and

(iii) limiting access to where no one can access after a specific number of readings of said message.

9. The method according to claim 7, wherein step (3) comprises the step of:

(b) setting a use limit including at least one step of the following steps:

(iv) limiting use to where no one can print said message,

(v) limiting use to where no one can archive said message, and

(vi) limiting use to where no one can cut/copy/paste said message.

10. The method according to claim 7, wherein step (3) comprises the step of:

(c) setting a receipt acknowledgment preference including the step of:

(vii) notifying the sender of receiver's opening of said message.

11. The method according to claim 7, wherein step (3) comprises the step of:

(d) setting a verification requirement including at least one step of the following steps:

(viii) setting verification of a personal identification number (PIN);

(ix) setting verification of a fingerprint;

(x) setting verification of a voiceprint;

(xi) setting verification of a digital signature;

(xii) setting verification of a retina scan;

(xiii) setting verification of a key;

(xiv) setting an auto self-destruct feature; and

(xv) setting a trip wire feature.

12. The method according to claim 7, further comprising the steps of:

(6) receiving said E-mail with said attachment at a receiver's computer;

(7) opening said E-mail and sending acknowledgment of receipt of said E-mail to the sender if requested;

(8) opening said attachment, activating attachment agents, and sending acknowledgment of attempted opening of said attachment to the sender if requested;

(9) determining whether criteria are satisfied to reveal said message; and

(10) revealing said message for viewing if said criteria in step (9) are determined to be satisfied including at least one step of the following steps:

(e) unencapsulating said message,

(f) sending acknowledgment of receipt of said message to the sender if requested,

(g) enforcing use limits, and

(h) enforcing access limits, and

unrevealing said message after viewing is complete.

13. The method according to claim 12, wherein step (9) further comprises the step of:

(j) determining if said access limits are exceeded;

(k) determining if said verification requirement is satisfied;

(l) instantiating a self-destruct agent if at least one of the following steps is satisfied:

(xvi) said access limits are determined to be exceeded in step (m), and

(xvii) said verification requirement is determined to not be satisfied and said auto self-destruct feature is set,

wherein said instantiating a self-destruct agent step includes at least one step of the following steps:

(xviii) overwriting file containing said E-mail and said message,

(xix) sending confirmation of self-destruction to the sender if requested, and

(xx) sending confirmation of self-destruction to the receiver if requested.

14. A method for enabling a sender to generate an encrypted E-mail for sending to a receiver, the method comprising the steps of:

(1) creating an E-mail with no content;

(2) attaching an attachment to said E-mail;

(3) preparing a message including setting an encryption feature;

(4) encapsulating said message in said attachment including encrypting said message; and

(5) sending said E-mail with said attachment from the sender to the receiver.

15. The method according to claim 14, wherein step (3) comprises the step of:

(a) setting an access limit including at least one step of the following steps:

(i) limiting access to where no one can access said message after a time duration after an event,

(ii) limiting access to where no one can access said message after an absolute date and time, and

(iii) limiting access to where no one can access after a specific number of readings.

16. The method according to claim 14, wherein step (3) comprises the step of:

(b) setting a use limit including at least one step of the following steps:

(iv) limiting use to where no one can print said message,

(v) limiting use to where no one can archive said message, and

(vi) limiting use to where no one can cut/copy/paste said message.

17. The method according to claim 14, wherein step (3) comprises the step of:

(c) setting a confirmation of self-destruct feature including at least one step of the following steps:

(vii) notifying the sender of self-destruction of the message, and

(viii) notifying the receiver of self-destruction of the message.

18. The method according to claim 14, further comprising the steps of:

(6) receiving said E-mail with said attachment at a receiver's computer;

(7) opening said E-mail;

(8) opening said attachment and activating attachment agents;

(9) determining whether criteria are satisfied to reveal said message; and

(10) revealing said message for viewing if said criteria in step (9) are determined to be satisfied including at least one step of the following steps:

(d) unencapsulating said message,

(e) unencrypting said message,

(f) enforcing use limits, and

(g) enforcing access limits, and

unrevealing said message after viewing is complete.

19. The method according to claim 18, wherein step (9) further comprises the step of:

(h) determining if said access limits are exceeded; and

(j) instantiating said self-destruct agent if said access limits are determined to be exceeded in step (h), including at least one step of the following steps:

(ix) overwriting file containing said E-mail and said message,

(x) sending confirmation of self-destruction to the sender if requested, and

(xi) sending confirmation of self-destruction to the receiver if requested.

20. A method for enabling a sender to generate a self-destructing, registered mail delivery and encrypted E-mail for sending to a receiver, the method comprising the steps of:

(1) creating an E-mail with no content;

(2) attaching an attachment to said E-mail;

(3) preparing a message including setting at least one of, a self-destruct feature, a registered mail delivery feature and an encryption feature;

(4) encapsulating said message in said attachment; and

(5) sending said E-mail with said attachment from the sender to the receiver.

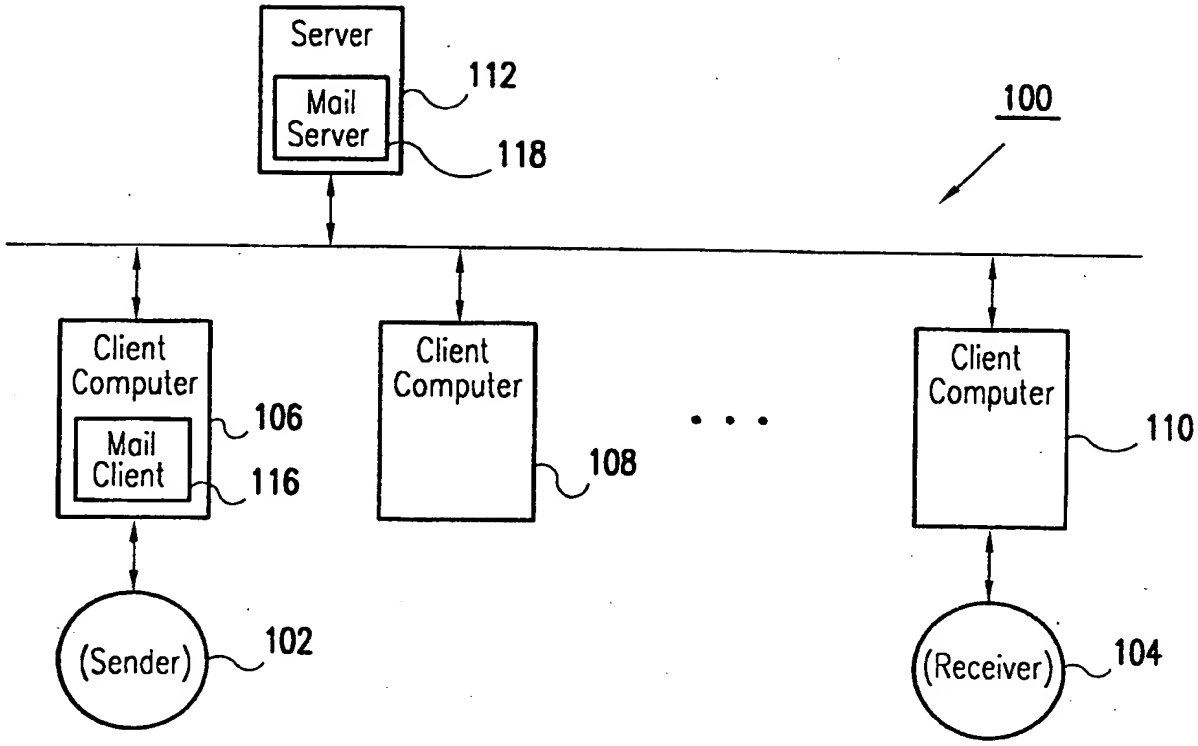



FIG.1A

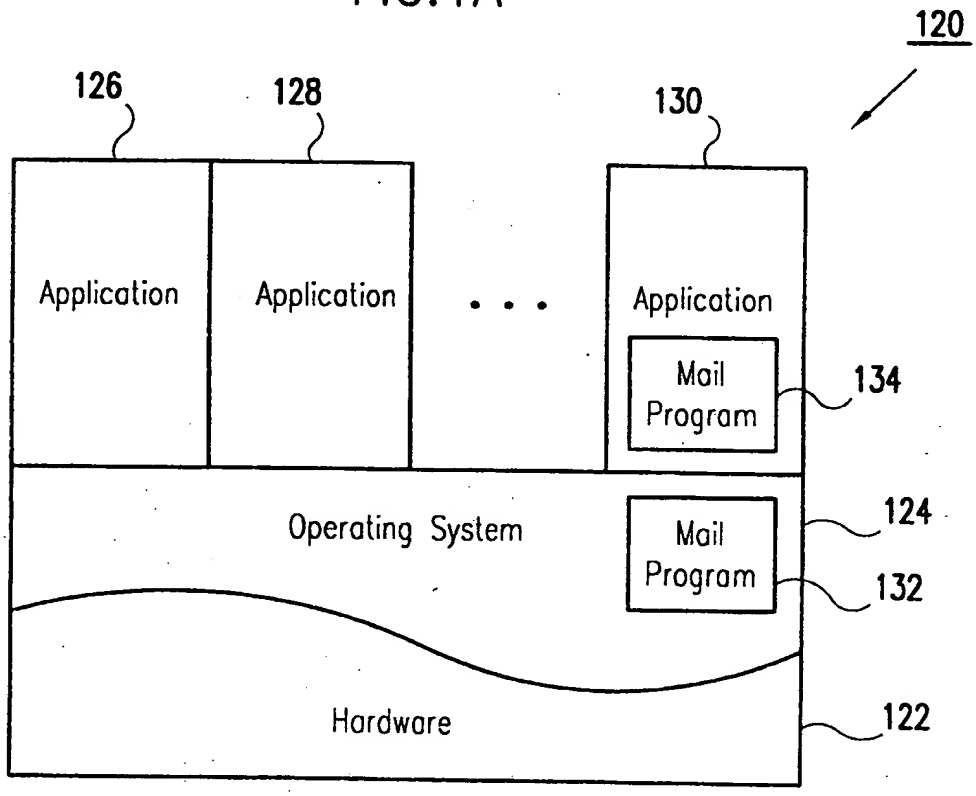



FIG.1B

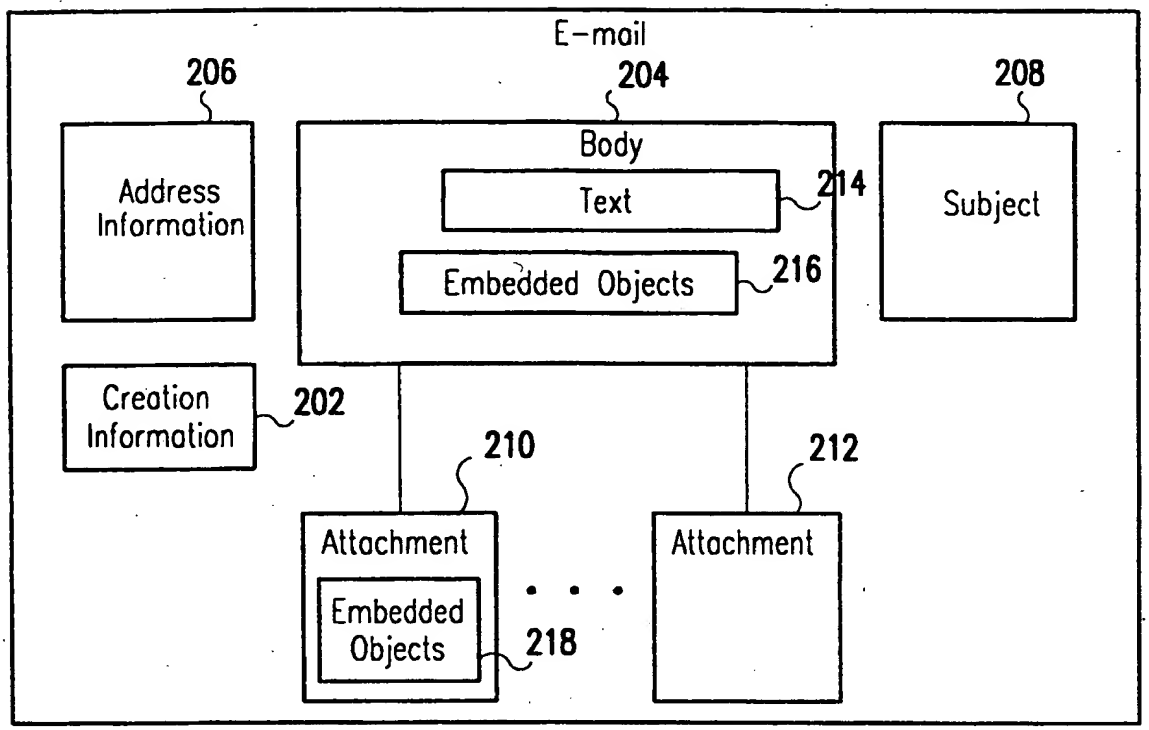



FIG.2A

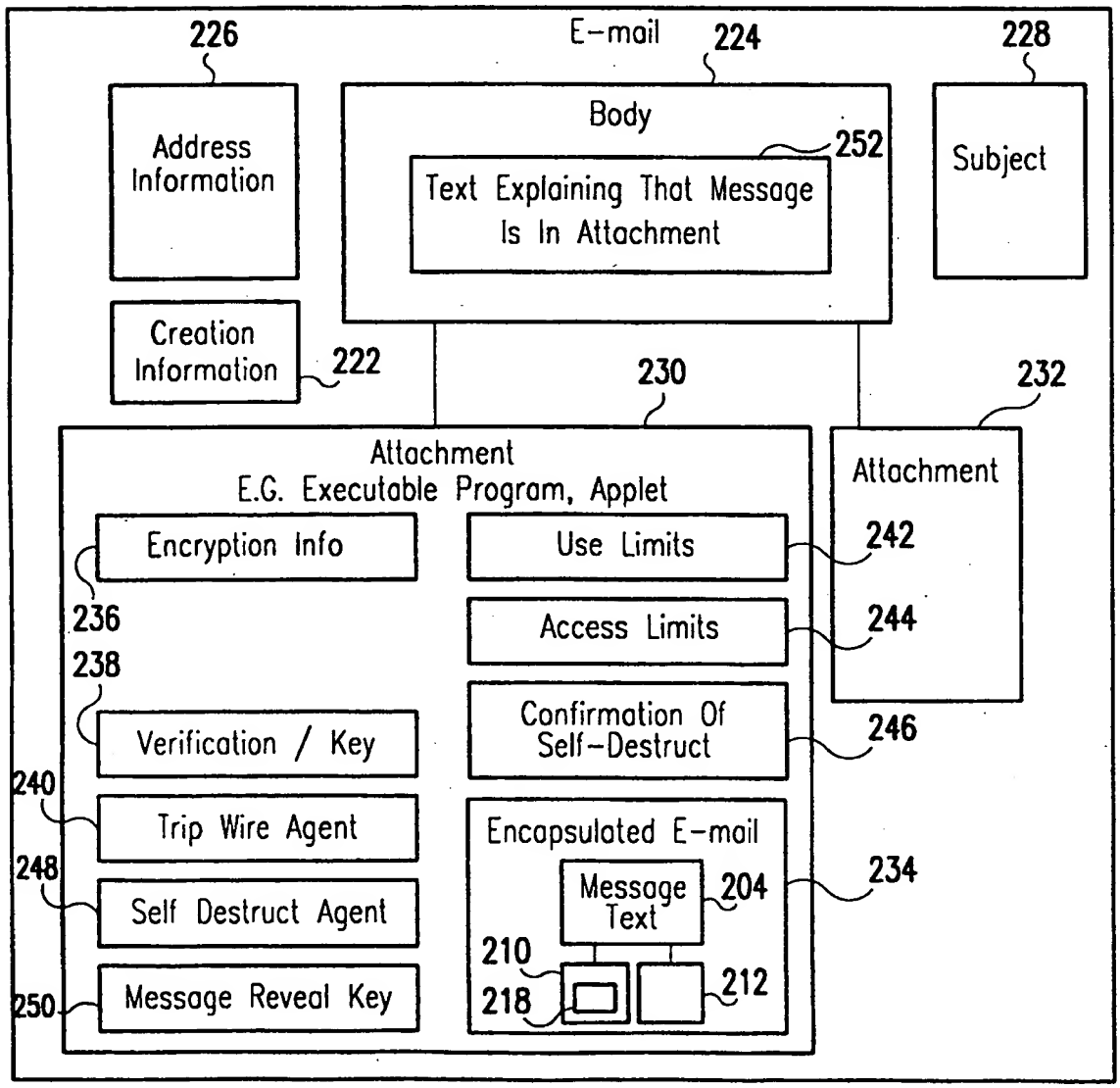



FIG.2B

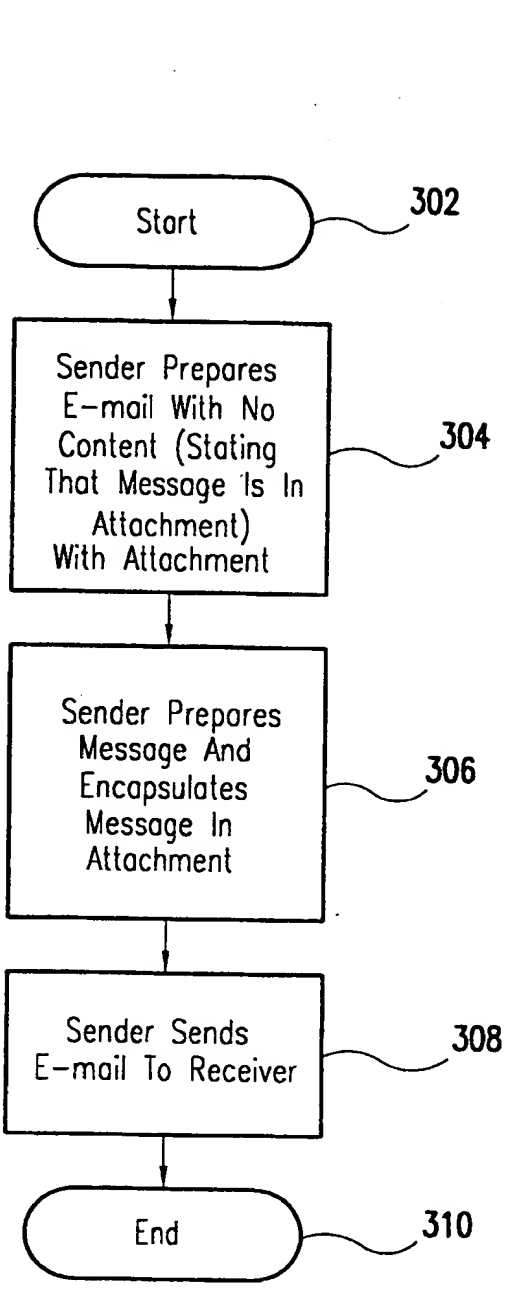



FIG.3

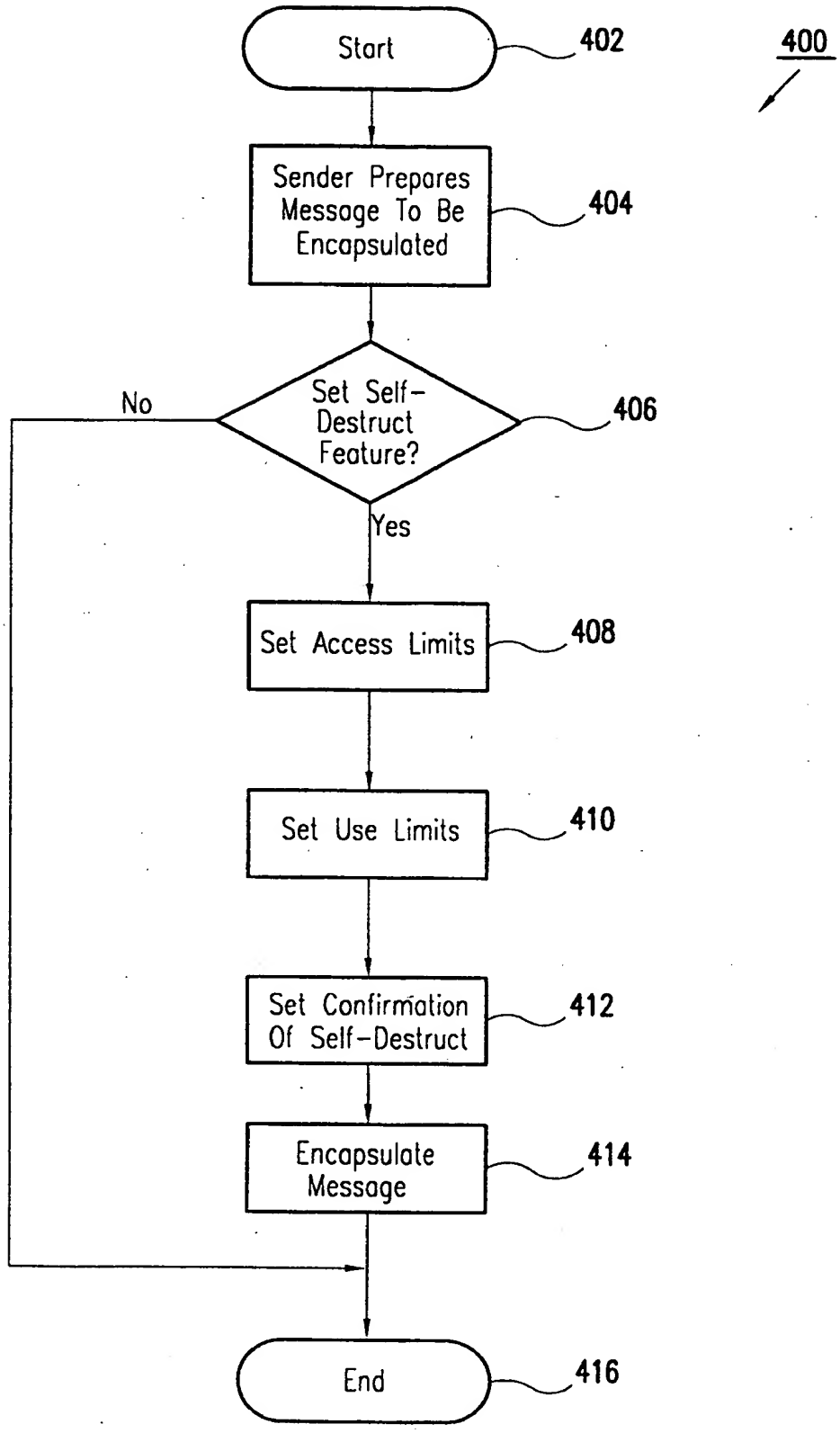



FIG.4

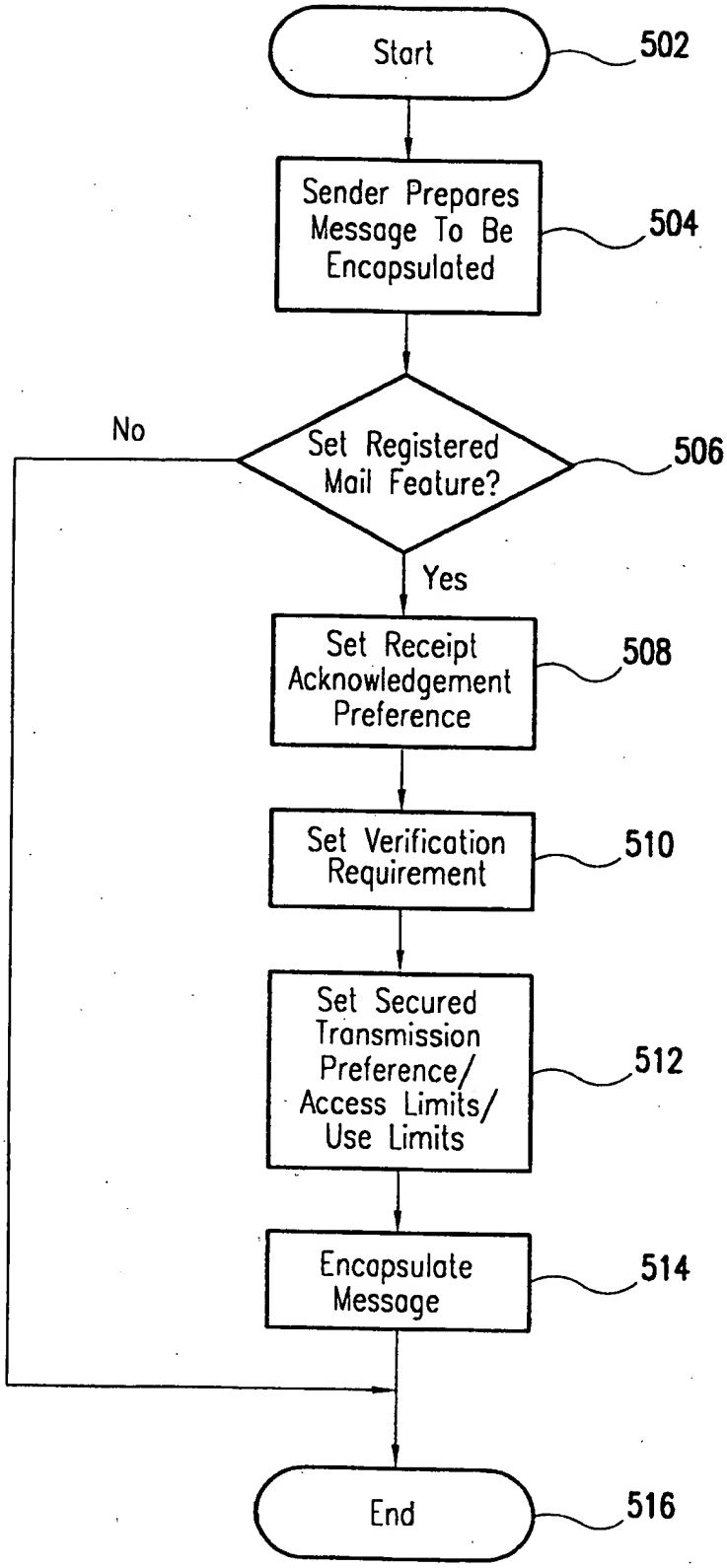



FIG.5

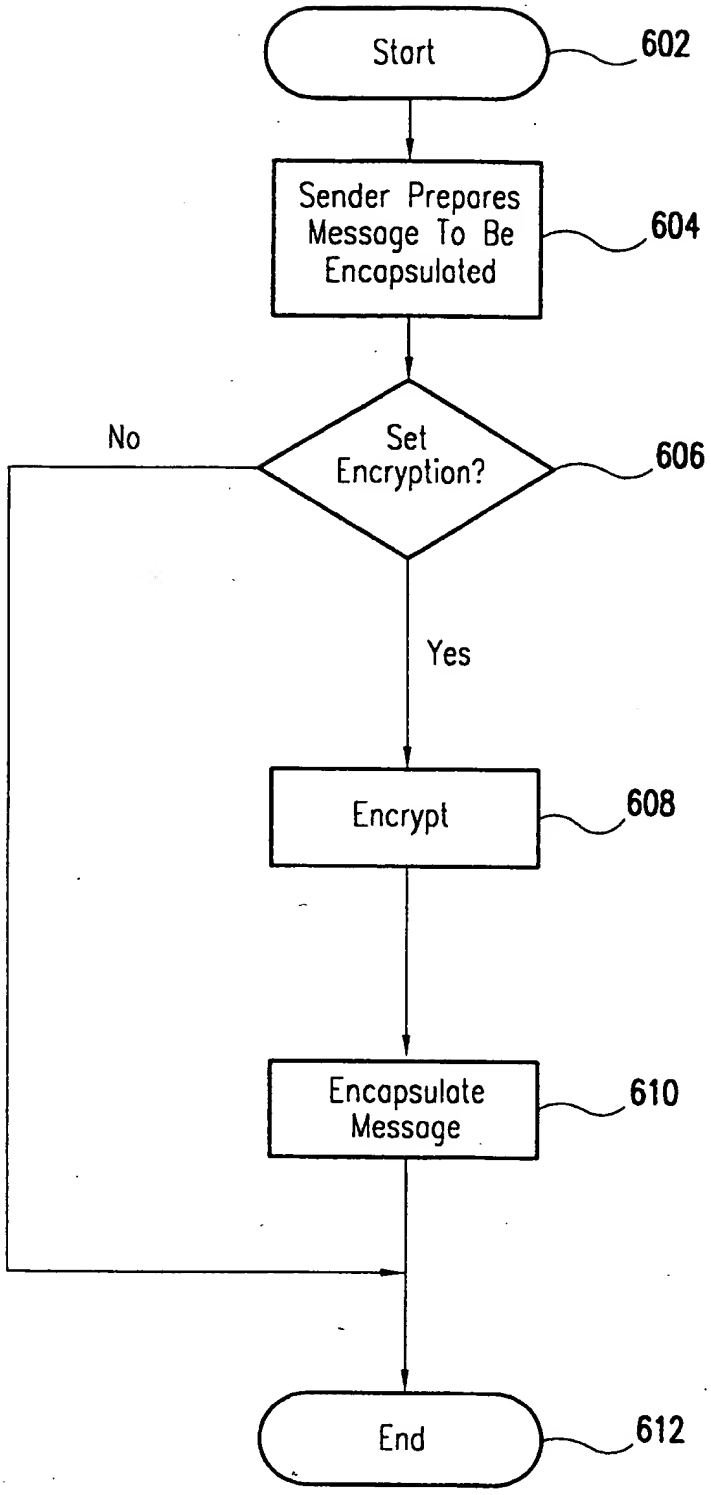



FIG.6

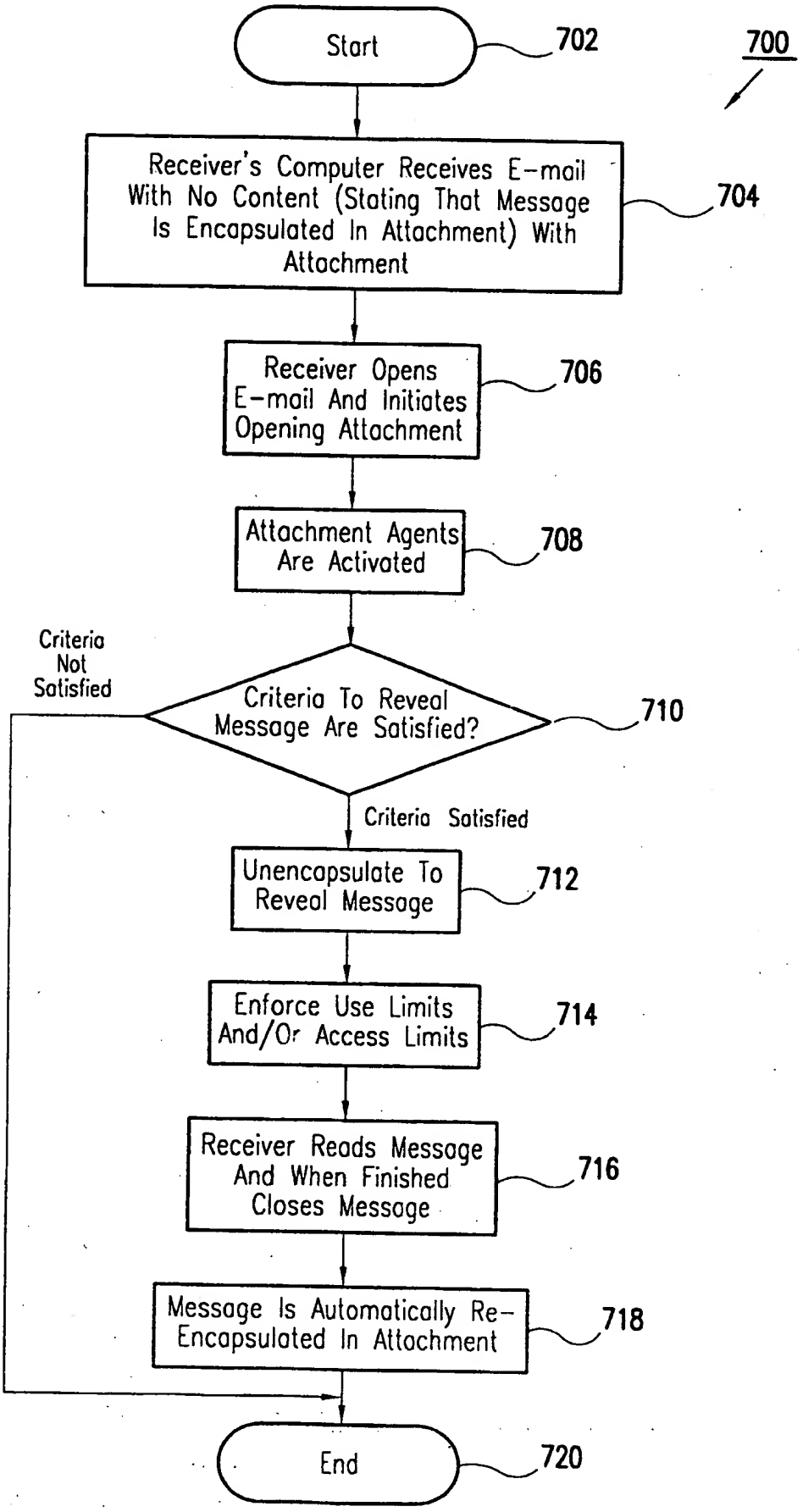



FIG.7

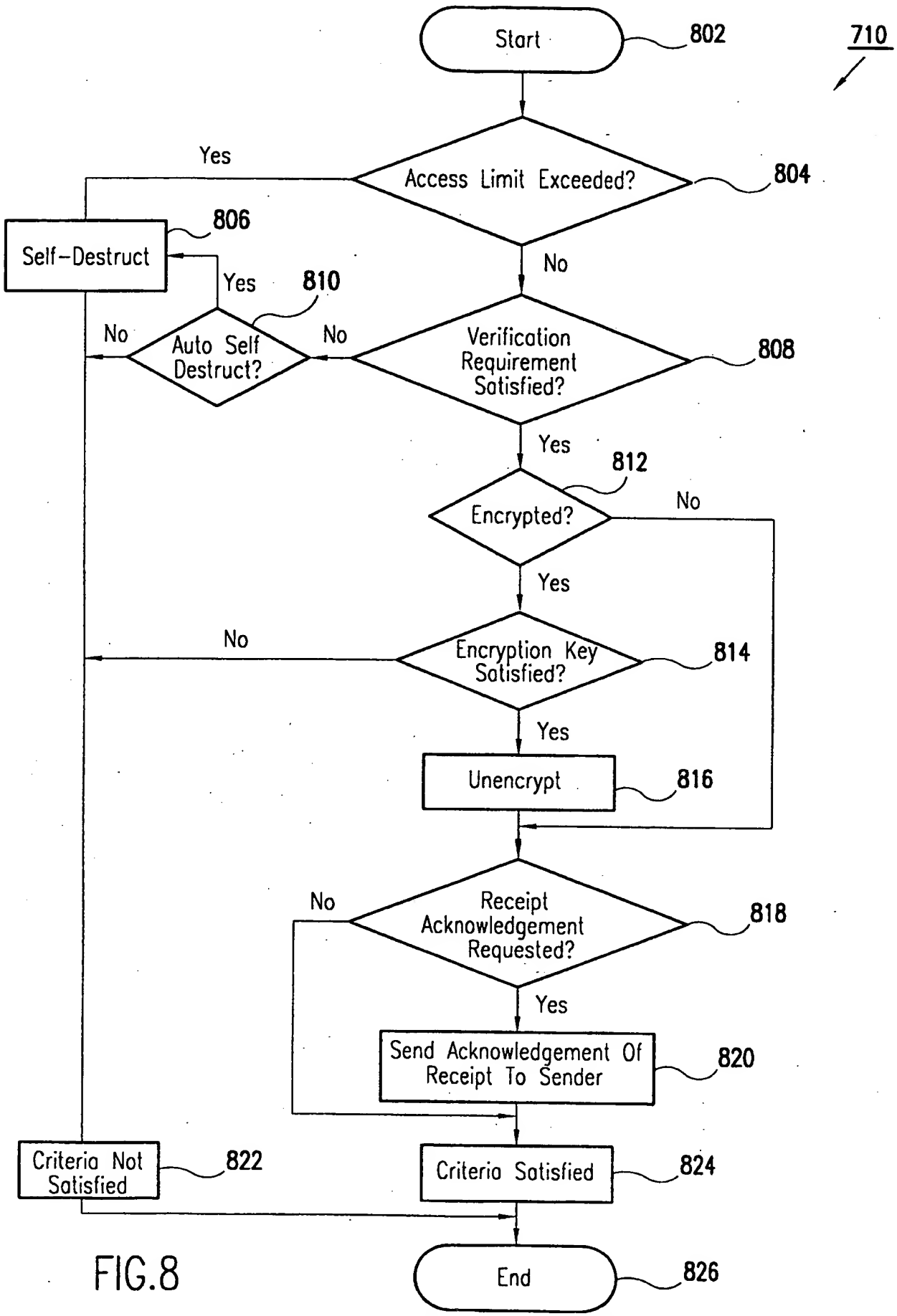



FIG.8

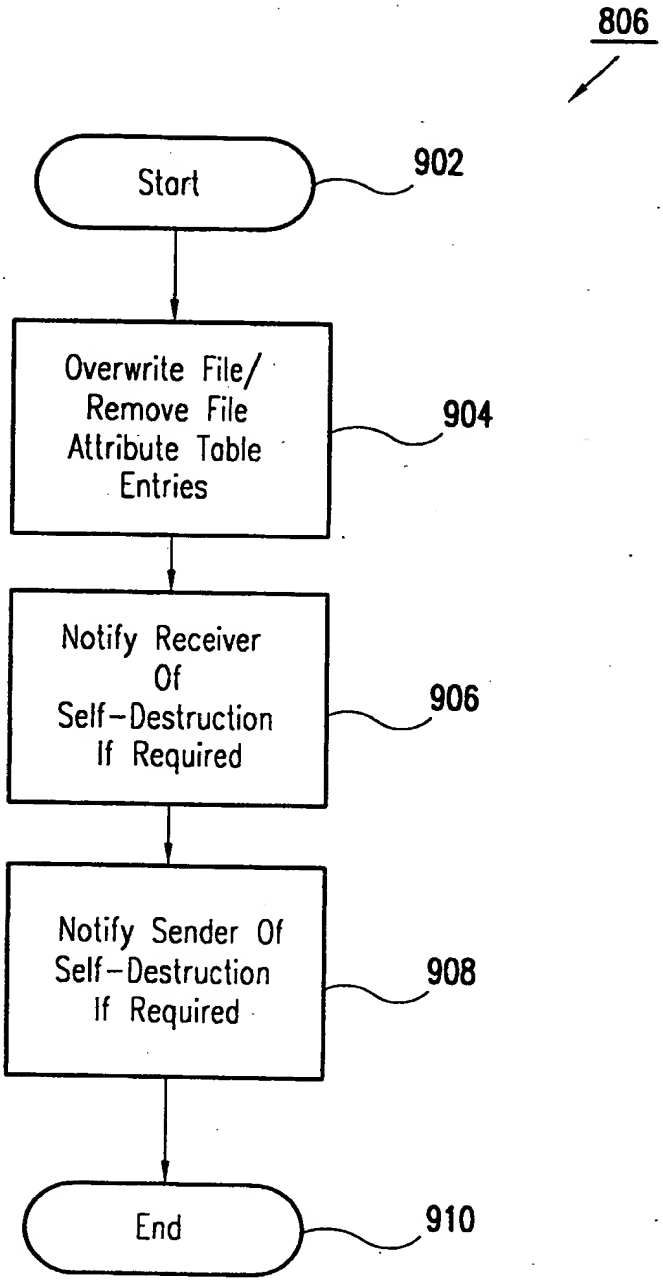



FIG.9

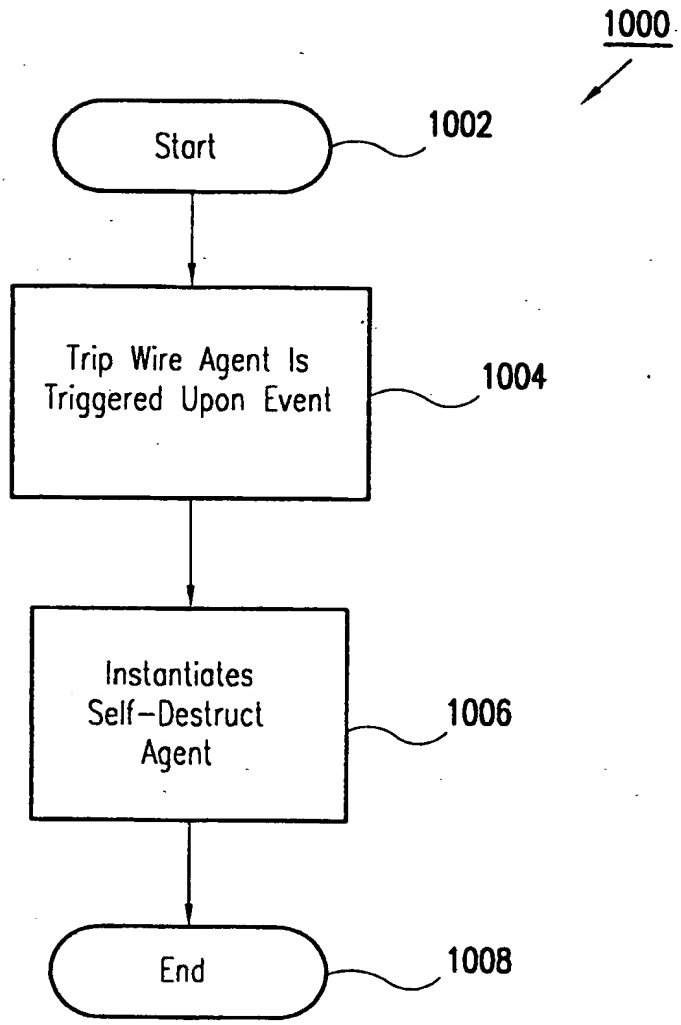



FIG.10

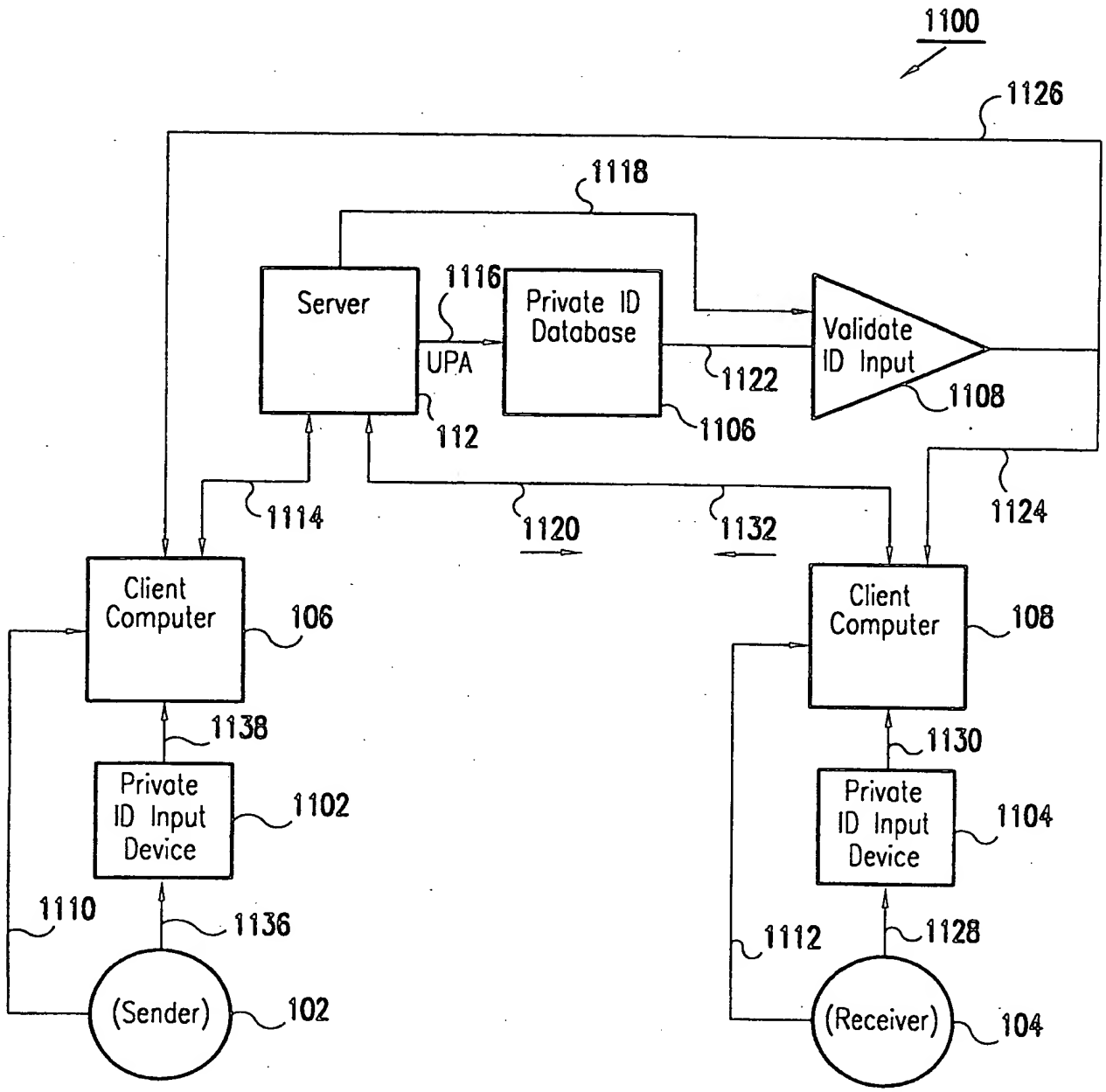



FIG.11

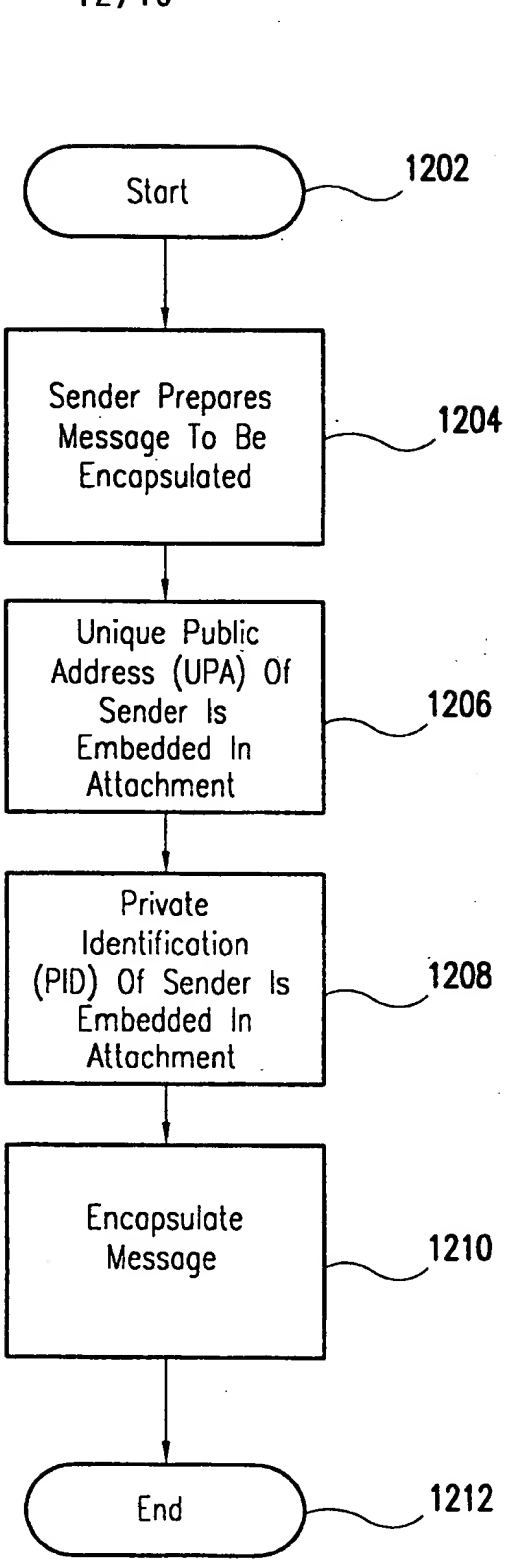



FIG.12

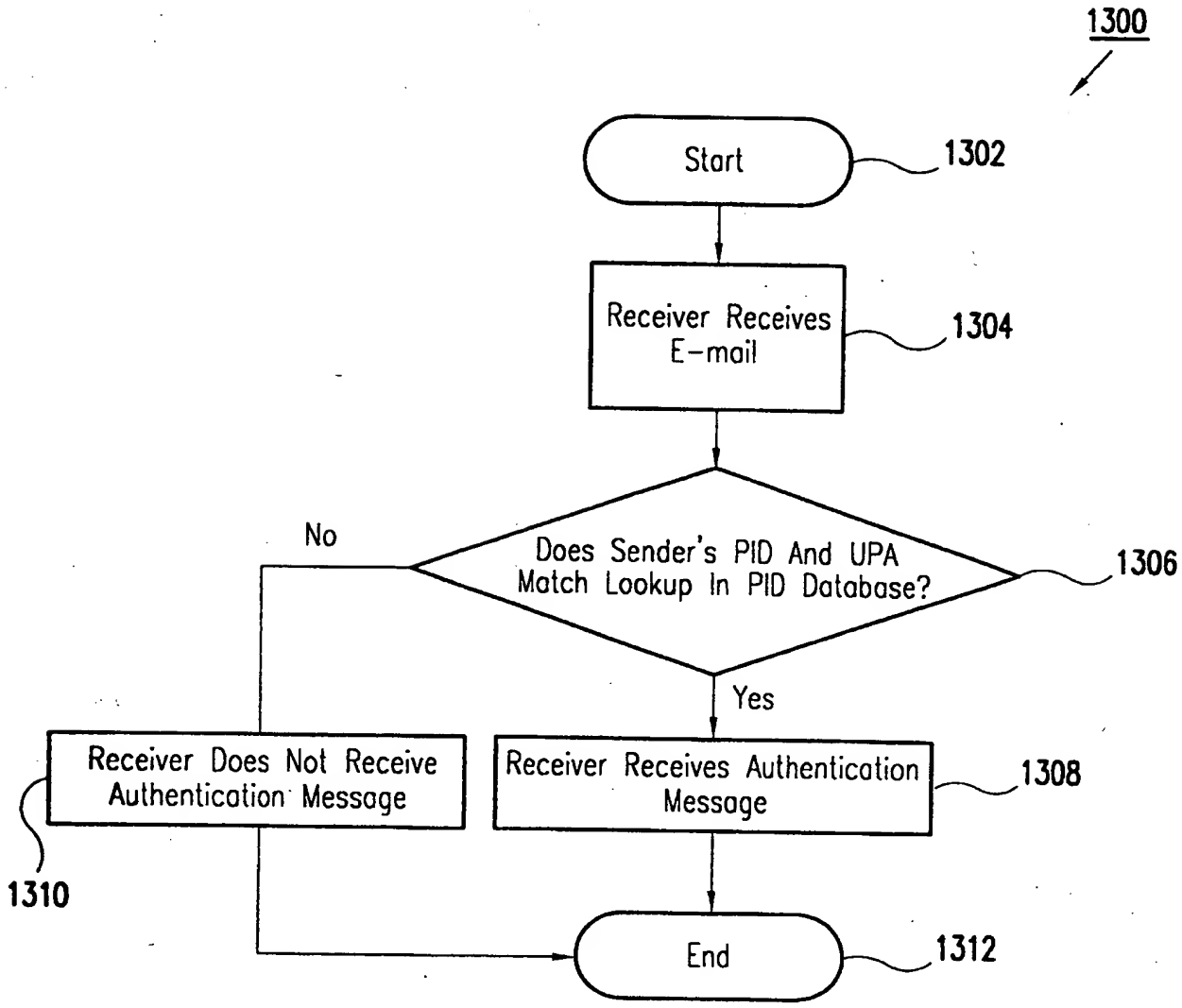



FIG.13

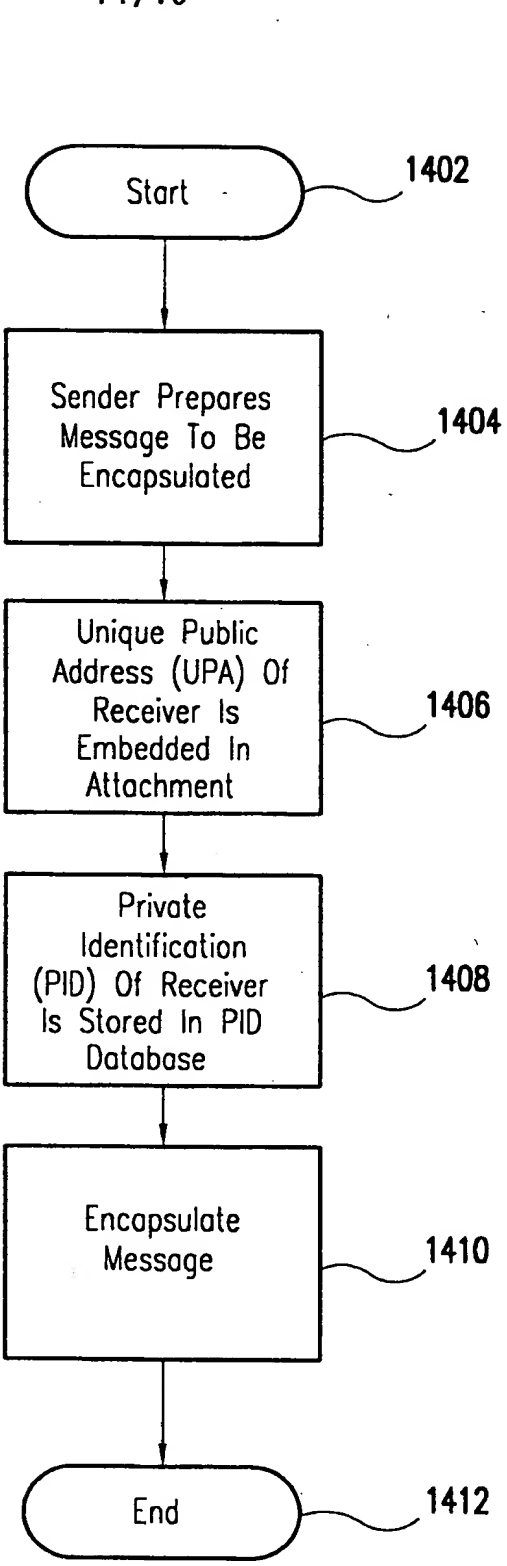



FIG.14

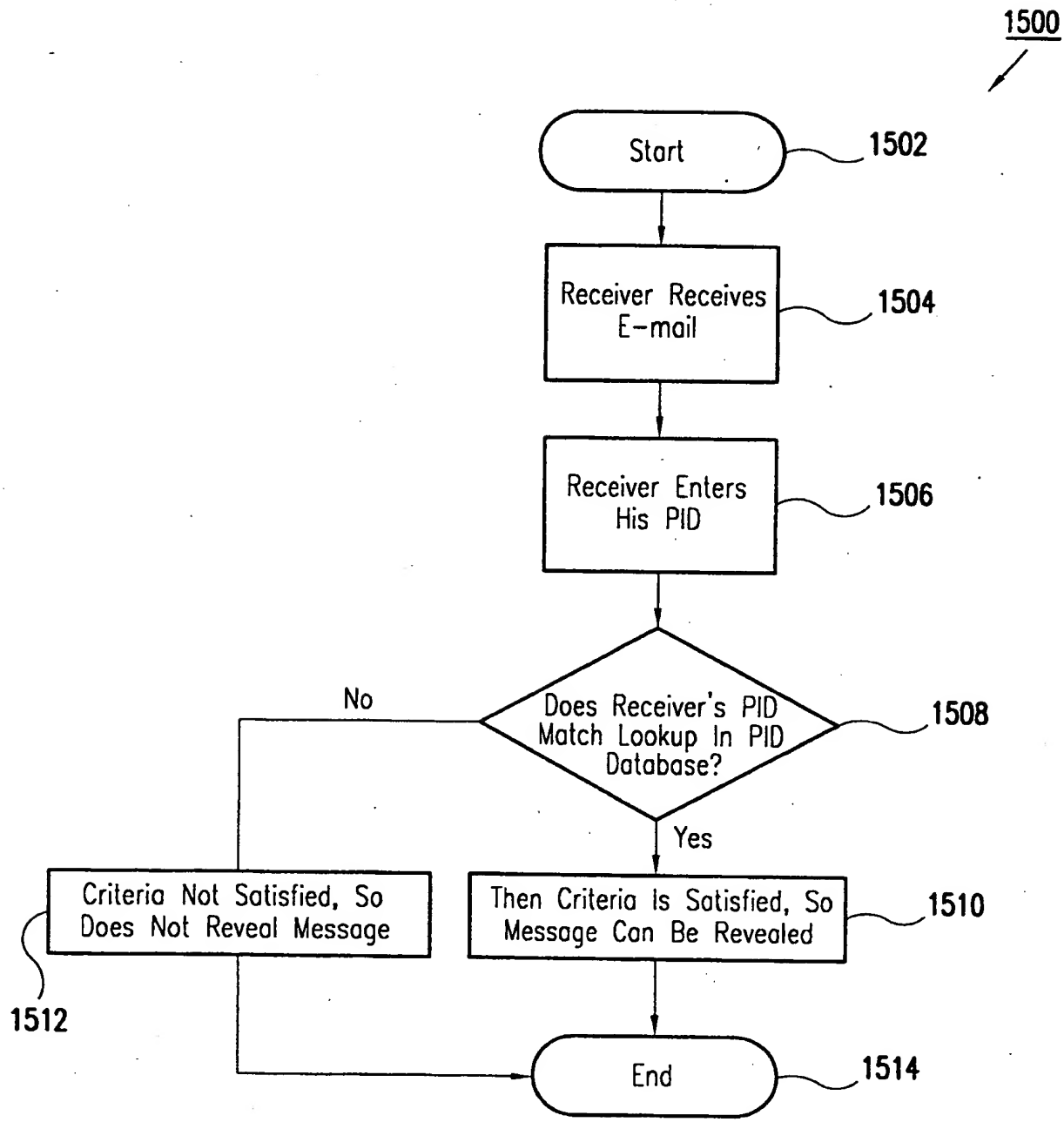



FIG.15

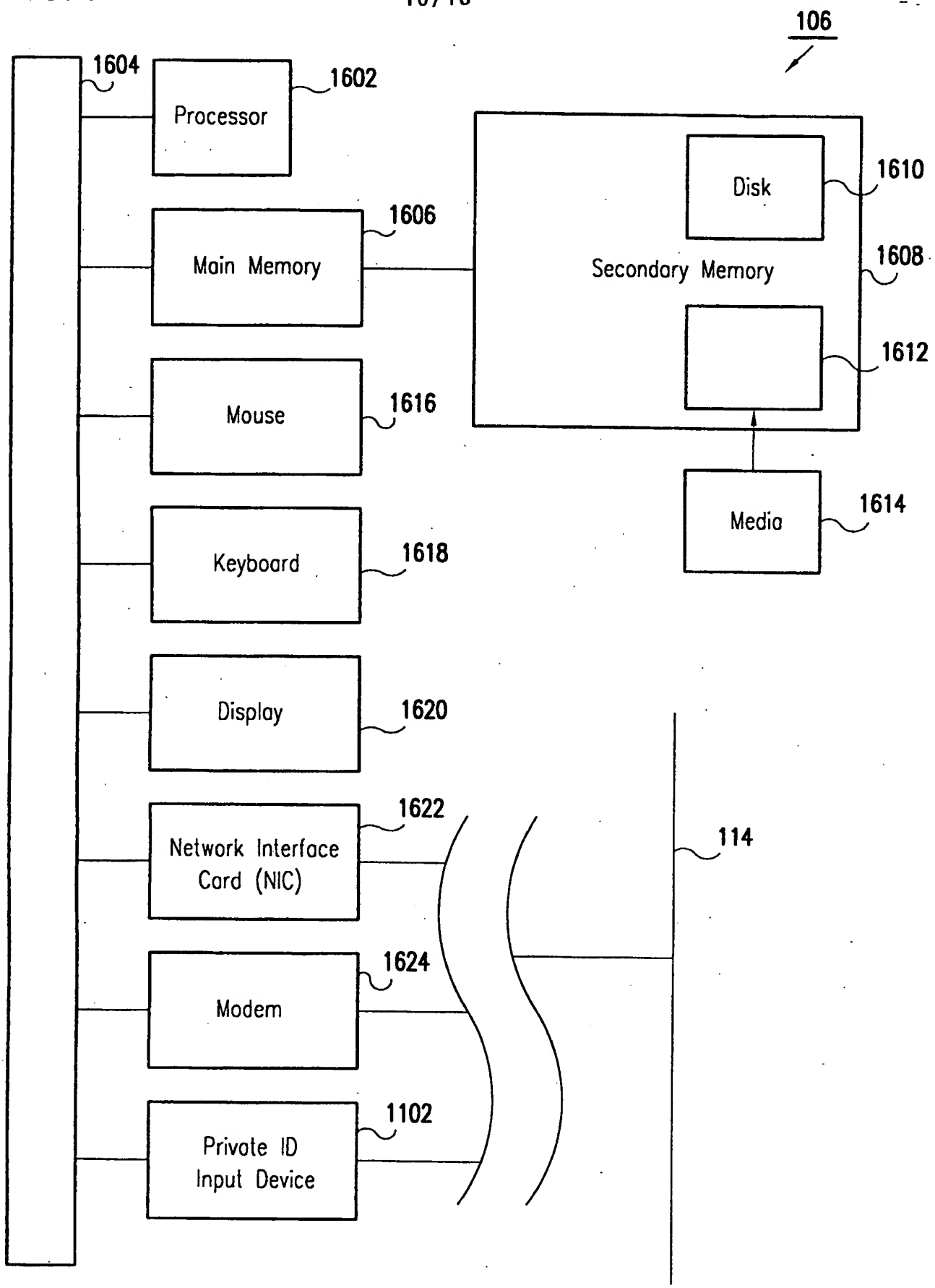



FIG.16

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/04723

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 17/30
US CL : 709/206, 202; 707/10; 713/201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/206, 202; 707/10; 713/201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
west

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A,P | US 5,958,005 A (THORNE et al) 28 September 1999 | 1-20 |
| A,P | US 5,917,489 A (THURLOW et al) 29 June 1999 | 1-20 |
| A | US 5,781,901 A (KUZMA) 14 July 1998 | 1-20 |
| A | US 5,325,310 A (JOHNSON et al) 28 June 1994 | 1-20 |
| A | US 5,014,234 A (EDWARDS, JR.) 07 May 1991 | 1-20 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | | | |
|---|---|---|---|
| * | Special categories of cited documents: | "T" | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| "A" | document defining the general state of the art which is not considered to be of particular relevance | "X" | document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| "E" | earlier document published on or after the international filing date | "Y" | document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" | document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" | document member of the same patent family |
| "O" | document referring to an oral disclosure, use, exhibition or other means | | |
| "P" | document published prior to the international filing date but later than the priority date claimed | | |

| | |
|---|---|
| Date of the actual completion of the international search<br>16 JUNE 2000 | Date of mailing of the international search report<br>03 JUL 2000 |
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703) 305-3230 | Authorized officer<br>GLENTON BURGESS Joni Hill<br>Telephone No. (703) 305-4792 |

Form PCT/ISA/210 (second sheet) (July 1998)*